2026-2027 PAYMENTS REGULATIONS:
Who's in Scope, What to Do, When It Hurts



Five regulatory changes will reshape the UK and EU payments ecosystem in the next 18 months. This handbook tells you which regimes actually apply to YOUR firm, what they demand, and which impressive-sounding acronyms you can safely ignore.

May 2026

Neira Jones

FOREWORD

If you work in payments, you already know the drill: every month brings another consultation, another acronym, another urgent webinar claiming this one will "change everything". Somewhere along the way it stopped being obvious which regimes really apply to your firm, and which are just background noise.

That is why I wrote this handbook.

The specific problem this document solves is simple: senior teams cannot see, in one place, which 2026-2027 regimes genuinely bite their business model, and which are noise for the next two years.

It does not try to catalogue every article and recital. Instead, it focuses on three things:

1. **Who** is actually in scope,
2. **What** they need to do,
3. **When** the real deadlines land.

If you are a UK-only PI with no EU footprint, you should not be spending evenings worrying about MiCAR. If you are a bank running Faster Payments volumes and safeguarding accounts, you absolutely should be thinking hard about APP fraud reimbursement and CASS 15.

I have tried to be explicit where a regime does not apply to you in 2026-2027, and equally explicit where it does, with enough detail to inform boards, CFOs and programme leads rather than only lawyers.

It is written to support one decision above all: how to sequence scarce change budget and board attention across CASS 15, PSD3, BNPL, crypto and EU AML Regulation, in line with the direction now set out in HM Treasury's Payments Forward Plan[1].

A short, but necessary disclaimer...

I am not a lawyer, and this document is not legal advice. It is a practitioner's synthesis of public rules and guidance as at February 2026, and it will not capture every nuance of your group structure, licences or products. It will however suggest when you should talk to your legal team.

So please use this roadmap as it is intended:

- **As a way to frame the questions you should be asking** your legal and compliance advisers.
- **As a tool to prioritise scarce change budget** and senior attention.
- **As a sense-check** on whether you are over-investing in the fashionable acronyms and under-investing in the regimes that actually carry deadlines, liability and authorisation risk.

If something in here makes you think "we might be in scope after all", the next step is not to quote this paper to your regulator. It is to pick up the phone to your lawyers and your supervisors and get clarity.

If, on the other hand, it helps you calmly decide that half the noise in your LinkedIn feed is not your problem for the next two years, it will have done its job. And if I have made some mistakes, please feel free to correct me and I'll make sure to publish updates!



Neira Jones

March 2026

HOW TO USE THIS HANDBOOK

Who, What, When?

This roadmap is structured to answer three critical questions:

1. **WHO** is impacted by regulatory changes?
2. **WHAT** must they do?
3. **WHEN** must they act?

IF YOU ARE...	READ THESE FIRST	2026 PRIORITIES TO LOOK FOR	SAFE TO IGNORE (UNTIL AFTER 2027)
UK-only PI/EMI (no EU, no crypto/BNPL)	Exec Dashboard; Chapter 1 (especially 1.1-1.4); Chapter 2 (2.2-2.4)	Implement CASS 15 by 7 May 2026; prepare for safeguarding audits; confirm CoP/APP fraud impact where relevant.	See Chapter 1, section 1.4 (BNPL, CRD/CRR and card-scheme rules you can park unless you expand into those roles).
UK PI/EMI with EU operations	Exec Dashboard; Chapters 1-2; Chapter 9 integration section	Implement UK CASS 15; run PSD3/PSR gap analysis and transition planning; choose safeguarding model (commercial banks vs central bank access).	Chapter 1, section 1.4 for non-payments regimes, plus Chapter 2, section 2.6 where risks are mainly for larger cross-border groups.
UK/EU BNPL lender	Exec Dashboard; Chapter 5 (5.2-5.5); Chapter 9 divergence section	Secure UK authorisation and CONC/SECCI/FOS readiness by 15 July 2026; implement EU CCD II market by market; prepare for AI/Consumer Duty/EU AI Act expectations.	Chapter 5, section 5.6 on what pure BNPL providers do not need to worry about in payments regulation.
Crypto firm with UK + EU footprint	Exec Dashboard; Chapter 4 (4.2-4.4); Chapters 1-2 if also a PI/EMI	Prepare and submit UK gateway application (30 Sep 2026-28 Feb 2027); embed MiCAR as business-as-usual; assess PSD3 and EU AML Regulation impact on any e-money-like stablecoins.	Chapter 4, introductory "What UK-only crypto firms do NOT need to worry about" box for MiCAR/PSD3 items that only bite if you go cross-border.
UK bank with Faster Payments/CHAPS	Exec Dashboard; Chapter 7 (7.2-7.5); Chapter 2 if a safeguarding bank	Continue to deliver CoP and APP fraud reimbursement; fulfil safeguarding-bank duties under CASS 15; implement UK MLR amendments and AI governance work.	Chapter 7, sections 7.1.1 and 7.1.2 highlight regimes that are not new implementation work in 2026-2027 (for example core prudential rules).
PISP/AISP-only open-banking provider (no PI/EMI licence)	Exec Dashboard; Chapter 3 (3.1-3.4); Chapter 9 AI/open banking sections.	Optimise access to bank APIs under current PSD2/UK PSRs; prepare for PSD3 access, NFC, and liability changes in the EU; assess agentic-AI use cases and governance where relevant.	Chapter 3, section 3.6 sets out what pure PISPs/AISPs can ignore, including safeguarding and EU AMLR if you are UK-only.
Acquirer	Exec Dashboard; Chapter 6 (6.1-6.3); Chapters 1-2 if you also hold PI/EMI licences; Chapter 7 if bank-licensed.	Confirm whether you hold merchant funds at end of day (safeguarding trigger); implement CASS 15 and PSD3 safeguarding if in scope; strengthen APP fraud, CoP/VoP, and operational-resilience arrangements.	Chapter 6, section 6.5 explains why most acquirers are out of scope for APP reimbursement and EU PSD3 safeguarding unless they also provide payment accounts or hold funds overnight.

If you play more than one role (for example PI plus acquirer, or bank plus BNPL), start with the Executive Dashboard and Stakeholder Impact Matrix, then read the chapters for each role and overlay their timelines into a single internal plan.

How to navigate this handbook

SECTION	WHAT'S IN IT FOR ME?
EXECUTIVE SUMMARY	**For the busy executive**. The two-page version of this handbook: what is changing, who genuinely needs to care, and the three things boards must sequence in 2026-2027 before the deadlines sequence them for you.
EXECUTIVE DASHBOARD	**For anyone building slides or running steering committees**. A lift-and-drop board pack page: heat map, Stakeholder Impact Matrix, and the 2026-2027 "calendar of pain" so you can see which regimes bite which roles, and when, without reading a full chapter.
CHAPTER 1 (PIs & EMIs)	**For PI/EMI boards, CFOs and programme leads**. Your primary map of which UK and EU regimes actually apply, which do not, and how CASS 15, PSD3, fraud and AMLR line up by business model and footprint.
CHAPTER 2 (Safeguarding)	**For safeguarding owners, COOs and treasury**. The CASS 15 and PSD3 safeguarding "how-to": what must be safeguarded, the seven-step CASS 15 routine, EU EMD2/PSD3 mechanics, and what different-sized firms must build by 7 May 2026 and then 2027-2028.
CHAPTERS 3 TO 8 (Other stakeholders)	**For leaders in open banking, crypto, BNPL, acquiring, banking and issuing**. One chapter per role with a requirements table, 2026-2027 action timeline, "what you do NOT need to worry about" boxes, and a short view of the people and effort you really need.
CHAPTER 9	**For group-level sponsors and portfolio owners**. The integration layer that shows how CASS 15, PSD3, BNPL, crypto, AMLR, AI and operational resilience interact across roles, where UK and EU are diverging, and how to turn the whole lot into one coherent change portfolio instead of seven siloed projects.
CONCLUSION	**For anyone asking "what now?"**. The joined-up view of how the regimes interact, where the UK and EU are converging or pulling apart, and the three non-negotiable actions you should take in 2026 if you want to be compliant and still in the market by 2028.

Contents

FOREWORD 2
HOW TO USE THIS HANDBOOK 3
Who, What, When? 3
How to navigate this handbook 4
EXECUTIVE SUMMARY 11
What is really changing 11
Who actually needs to care 11
What you must do in 2026 - and what can wait 12
How to use this roadmap without drowning in it 12
EXECUTIVE DASHBOARD 13
1. Regulatory Change Heat Maps 13
HIGH IMPACT Changes 13
MEDIUM IMPACT Changes 14
LOW IMPACT Changes 15
2. Stakeholder Impact Matrix 16
3. Critical Milestone Timeline 17
Chapter 1: Payment Institutions & E-Money Institutions 18
1.1 Regulatory Requirements: PIs vs EMIs (Consolidated Table) 19
1.2 Priority Action Timeline: PIs & EMIs (UK & EU) 20
1.3 Building your PI/EMI roadmap (UK & EU 20
1.4 What PIs and EMIs do not need to worry about in 2026-2027 21
1.4.1 BNPL Regulation (Buy Now Pay Later) 21
1.4.2 CRD IV/CRR Prudential Regime 21
1.4.3 Card Scheme Rules (Visa/Mastercard) 21
Chapter 2: Safeguarding Requirements for PIs & EMIs 22
2.1 Safeguarding Requirements Comparison Tables 22
2.1.1 Generic principles 22
2.1.2 PIs and EMIs: UK vs. EU requirements (current and near-term) 23
2.2 UK Safeguarding (CASS 15) 24
2.2.1 What PIs Must Safeguard (UK) 24
2.2.2 What EMIs Must Safeguard (UK) 24
2.2.3 CASS 15 Core Requirements (UK) 25
2.2.4 Implementation Timeline (UK CASS 15) 26
2.3 EU E-Money Safeguarding (EMD2 & PSD3 Transition) 27
2.3.1 Current EU E-Money Safeguarding (EMD2 - pre-PSD3) 27
2.3.2 EU Payment Institution Safeguarding (PSD2 - pre-PSD3) 28

2.3.3 PSD3/PSR Safeguarding Framework (Post-Q4 2027) 28
2.3.4 Central Bank Safeguarding Access (PSD3 Opportunity) 29
2.4 Priority Actions by Jurisdiction 29
2.4.1 UK (CASS 15 - Deadline 7 May 2026) 29
2.4.2 EU (Current EMD2/PSD2 - Monitor for PSD3 Transition) 30
2.5 Resource Requirements by Firm Size 30
2.5.1 Small PIs/EMIs (< £50M annual payment volume) 30
2.5.2 Medium PIs/EMIs (£50M-£250M annual payment volume) 31
2.5.3 Large PIs/EMIs (> £250M annual payment volume) 31
2.5.4 Resourcing Recap 31
2.6 Risk Factors & Mitigation 32
2.6.1 Operational Risks 32
2.6.2 Regulatory Risks 32
2.6.3 Strategic Risks 32
Chapter 3: PISPs & AISPs (Open Banking Providers) 33
3.1 Regulatory Requirements Comparison Table 33
3.2 Current Regime: UK PSRs (retained PSD2) and EU PSD2 34
3.3 Post-PSD3 Regime: Enhanced Rights (EU only) 34
3.3.1 Stronger Access Obligations on Banks (PSD3) 34
3.3.2 Mobile Operating System Access (PSD3) 35
3.3.3 Clarified Liability Framework (PSD3) 35
3.3.4 Agentic AI Implications (If Applicable) 36
3.4 Priority Action Timeline 37
UK PISPs/AISPs (Q1-Q4 2026) 37
EU PISPs/AISPs (Q2 2026-Q4 2027) 37
3.5 Resource Requirements 39
Small PISPs/AISPs (< 100k users) 39
Large PISPs/AISPs (> 1M users) 39
3.6 Out of Scope for PISPs/AISPs 39
What PISPs/AISPs do NOT need to worry about: 39
What UK-only PISPs/AISPs do NOT need to worry about in 2026-2027 39
3.7 Risk Factors & Mitigation 40
Regulatory Risks 40
Operational Risks 40
Strategic Risks 40
3.8 Key Takeaways 41
Chapter 4: Cryptoasset Firms 42
4.1 Regulatory Requirements Comparison Table 43

4.2 UK Crypto Regime (FSMA 2023) 44
4.2.1 Authorisation Categories 44
4.2.2 UK Gateway Process (CRITICAL) 45
4.2.3 Application Preparation (Critical Path) 46
4.2.4 Life After Authorisation: Ongoing Obligations 46
4.3 EU MiCAR Regime 47
4.3.1 UK vs. EU Detailed Comparison 47
4.3.2 MiCAR Categories 48
4.3.3 Key Compliance Obligations (EU) 49
4.3.4 PSD3 Interaction (EU Stablecoin Issuers Only) 50
4.4 Priority Action Timeline 51
4.4.1 All Crypto Firms (Q1-Q3 2026 - UK and EU) 51
4.4.2 UK Crypto Firms (Q3-Q4 2026) 51
4.4.3 EU Crypto Firms (Q2 2026-Q4 2027) 51
4.4.4 All Crypto Firms (2027 Ongoing) 51
4.5 Resource Requirements 52
4.5.1 Small Crypto Firms (< £10M annual volume) 52
4.5.2 Large Crypto Firms (> £500M annual volume) 52
4.5.3 Dual UK/EU firms 52
4.6 Critical Success Factors 53
4.7 Risk Factors & Mitigation 53
Regulatory Risks 53
Operational Risks 54
Reputational Risks 54
4.8 Key Takeaways 54
Chapter 5: BNPL Providers 55
5.1 Regulatory Requirements Comparison Table 55
5.2 UK BNPL Regulation (FCA) 57
5.2.1 Authorisation Requirement 57
5.2.2 Creditworthiness Assessments (CONC 5.2A) 58
5.2.3 Pre-Contract Information (SECCI Form) 59
5.2.4 Adequate Explanations 59
5.2.5 Merchant Exemption (UK-specific) 60
5.2.6 Financial Ombudsman Service (FOS) Jurisdiction 60
5.3 EU BNPL Regulation (Consumer Credit Directive) 61
5.4 Priority Action Timeline 62
UK BNPL Providers (Q1-Q3 2026) 62
EU BNPL Providers (Q2-Q4 2026) 62

All BNPL Providers (Q4 2026-2027) 62
5.5 Resource Requirements 63
Small BNPL Providers (< £50M credit outstanding) 63
Large BNPL Providers (> £500M credit outstanding) 63
Dual UK/EU Providers: 63
5.6 Out of Scope for BNPL Providers 63
5.7 Risk Factors & Mitigation 64
Regulatory Risks 64
Operational Risks 64
Reputational Risks 64
5.8 Key Takeaways 65
Chapter 6: Acquirers 66
6.1 Regulatory Requirements Comparison Table 67
6.2 Three Acquirer Business Models Detailed 68
6.2.1 Model A: Bank-Licensed Acquirers 68
6.2.2 Model B: PI-Licensed Acquirers (Payment Institution) 69
6.2.3 Model C: EMI-Licensed Acquirers (E-Money Institution) 70
6.3 Priority Action Timeline 71
All Acquirers (Q1 2026 - Immediate) 71
Model B (with fund holding) / Model C Acquirers (Q1-Q2 2026) 71
All Acquirers (Q2-Q4 2026) 71
6.4 Resource Requirements 72
6.4.1Model A (Bank-Licensed, no safeguarding) 72
6.4.2 Model B (PI, no fund holding) 72
6.4.3 Model B (PI, with fund holding) 72
6.4.4 Model C (EMI-Licensed) 72
6.5 Out of Scope for Acquirers 73
6.6 Risk Factors & Mitigation 73
Regulatory Risks 73
Operational Risks 73
Reputational Risks 73
6.7 Key Takeaways 74
Chapter 7: Banks (ASPSPs) 75
Introduction 75
7.1 Regulatory Requirements Comparison Tables 75
7.1.1 UK banks: regulatory requirements (current and near-term) 75
7.1.2 EU banks: regulatory requirements (current and near-term) 76
7.1.3 What 2026-2027 really means for banks 77

7.2 UK: Fraud, safeguarding-bank role and resilience 78
7.2.1 Confirmation of Payee (CoP) 78
7.2.2 APP Fraud Reimbursement (Faster Payments & CHAPS) 79
7.2.3 Operational Resilience Reporting & Incident Management 80
7.2.4 Role as Safeguarding Bank (for PIs/EMIs) 81
7.2.5 Open Banking API Access (PISPs/AISPs) 82
7.2.6 Consumer Duty (payments and fraud) 83
7.2.7 UK Money Laundering Regulations (MLRs) - 2024 Amendments 84
7.3 EU: PSD3, VoP, AMLR and AI Act 85
7.3.1 Verification of Payee (VoP) 85
7.3.2 PSD3 Fraud Prevention & Spoofing Liability 86
7.3.3 PSD3 Open Banking Access 87
7.3.4 PSD3 Consumer Protection & Spending Limits 88
7.3.5 EU Anti-Money Laundering Regulation (AMLR) 89
7.4 Priority Action Timeline 90
UK banks (Q1 2026-Q4 2027 & Beyond) 90
EU Banks (Q1 2026-Q4 2027) 90
7.5 Resource Requirements by Bank Size 91
Small/Regional Banks (< £50B total assets) 91
Large Banks (£50B-£500B total assets) 91
Systemically Important Banks (> £500B total assets) 91
7.6 Risk Factors & Mitigation 92
Regulatory Risks 92
Operational Risks 92
Strategic Risks 92
Chapter 8: Card Issuers 93
8.1 Regulatory Requirements Comparison Table 94
8.2 UK-Specific Requirements for Card Issuers 95
8.2.1 FCA Consumer Duty & Credit Decisioning 95
8.2.2 Fraud Detection & De-Banking Risk 95
8.2.3 Operational Resilience (if systemically important) 96
8.3 EU-Specific Requirements for Card Issuers 96
8.3.1 PSD3 Strong Customer Authentication (SCA) - Outcomes Based 96
8.3.2 PSD3 Fraud Liability & Spoofing 96
8.3.3 PSD3 Consumer Protection & Spending Limits 97
8.3.4 EU AI Act (December 2027) 97
8.4 Priority Action Timeline 97
UK Card Issuers (Q1-Q4 2026) 97

EU Card Issuers (Q1 2026-Q4 2027) 97
8.5 Resource Requirements 98
UK Card Issuers 98
EU Card Issuers 98
8.6 What card issuers do NOT need to worry about 98
Safeguarding Obligations 98
APP Fraud Reimbursement 99
BNPL Regulation 99
8.7 Risk Factors & Mitigation 99
Regulatory Risks 99
Operational Risks 99
8.8 Key Takeaways 99
Chapter 9: Regulatory Divergence & Critical Integration Points 100
9.1 UK vs EU Divergence at a Glance 100
9.2 Integration & Interaction: How Stakeholders Intersect 100
9.2.1 Payment Institutions + Acquirers (Fund Holding Risk) 100
9.2.2 PISPs + Banks (API Dependency) 101
9.2.3 Stablecoin Issuers + PSD3 (Dual Compliance Risk) 101
9.3 How to organise the work 101
9.3.1 Recommended governance for medium/large firms: 101
9.3.2 Recommended governance for small firms: 102
Conclusion: The 2026-2027 Regulatory Reckoning 103
The Strategic Imperative 103
Integration & Interaction: How the Pieces Combine 103
Three Non-Negotiable Actions (2026) 103
The Bottom Line 103
REFERENCES 105

EXECUTIVE SUMMARY

2026-2027 is when "nice-to-know" regulation turns into hard stop dates. This roadmap is your cheat sheet for which regimes actually bite your firm, where, and when - and which impressive-sounding acronyms you can safely ignore.

What is really changing

Five regimes do most of the damage in the next 18-24 months:

- CASS 15 (UK safeguarding) makes daily reconciliation, audits, and resolution packs non-negotiable for UK PIs/EMIs by 7 May 2026[2].
- UK BNPL rules drag third-party BNPL into full FCA authorisation and affordability checks from 15 July 2026[3].
- PSD3/PSR[4] finally harden into reality, with EU PSPs facing late-2027/2028 application after an 18-21 month transition.
- UK cryptoasset authorisation is now fixed in law: the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 bring in-scope cryptoasset activities into the FCA's FSMA remit, with a gateway window for existing firms from 30 September 2026 to 28 February 2027, and the new regime expected to apply from 25 October 2027, turning "let's see" into "authorised or exit".
- EU AML Regulation (AMLR) goes live on 10 July 2027[5], adding an EU-level AML supervisor on top of national regimes.

Everything else - AI Acts, DORA evolutions, post-quantum standards - is important, but more "turn the ship now" than "hit the iceberg this quarter".

HM Treasury's Payments Forward Plan, developed with the Payments Vision Delivery Committee, now sets a public 2026-2028 roadmap for payments reforms, consolidation of the Payment Systems Regulator (PSR) into the Financial Conduct Authority (FCA), and further work on stablecoins; this handbook is written to help individual firms turn that high-level plan into a concrete delivery sequence.

Who actually needs to care

The document is ruthless about scope:

- **PIs/EMIs**: Must care about CASS 15, PSD3 safeguarding and fraud, CoP/VoP, APP fraud, the EU AML Regulation, and - if they hold e-money-like stablecoins - PSD3/MiCAR overlap. They do not need to lose sleep over CRD/CRR or card-scheme minutiae unless they are also acquirers or issuers.
- **PISPs/AISPs**: Live and die on bank API quality. PSD3 turns EU banks from gatekeepers into infrastructure, but UK-only PISPs stay in today's PSD2 mud. Safeguarding is someone else's problem.
- **Crypto firms**: UK-only players are on a single-track journey to FSMA authorisation[6]; EU operators are already in MiCAR[7] and may pick up PSD3 and the EU AML Regulation as a second regulatory language.
- **BNPL providers**: Sit firmly in the consumer-credit world, not the payment-services world. They get their own regimes in the UK and EU, plus AI governance and FOS/ombudsman scrutiny, but no CASS 15 or PSD3.
- **Acquirers, issuers, and banks**: Feel the real pain in fund-holding classification, fraud liability and safeguarding-bank duties, not "yet another alphabet soup". A T+0 bank acquirer is in a different universe from an EMI-acquirer that runs merchant balances as e-money.

If you are UK-only and don't touch BNPL, crypto or EU customers, a surprising amount of the noise genuinely does not apply to you.

What you must do in 2026 - and what can wait

Three themes demand board-level attention now:

1. **Get your business model classification right**: Whether you hold funds, where, and for whom multiplies your regulatory burden by a factor of five to ten. Misclassification discovered after the fact means remediation, not sympathy.
2. **Use the gateway windows or lose the market**:
   - BNPL authorisation and CONC enforcement hit in mid-2026.
   - Crypto firms that don't get into the UK gateway[8] between September 2026 and February 2027 will be choosing between rushed exits and emergency applications.
3. **Start PSD3 preparation before the ink dries**: Waiting for every technical standard is a good way to meet the deadline with a remediation plan instead of a working platform.

Everything else - AI governance, EU AI Act[9], post-quantum - is best treated as structured change workstreams, not fire drills: design a target governance model once, then use it repeatedly.

How to use this roadmap without drowning in it

The document is built for skimming and slicing:

- Start with the heat map and "Most relevant for" lines to find your regimes.
- Use the Stakeholder Impact Matrix to confirm what really applies to your roles.
- Go to the chapter for each role you play (PI, EMI, acquirer, bank, BNPL, crypto, PISP/AISP, issuer) and pull out the timelines and "do not worry about" boxes.
- Overlay the timelines into a single internal plan; for hybrid firms, that usually means one safeguarding programme, one fraud/APP/PSD3 programme, and one AI/operational-resilience programme.

If you do this, 2026-2027 becomes a controlled transformation, not a regulatory pile-up. If you do not, the regulators will be very happy to help you prioritise, one Dear CEO letter at a time.

Most horizon-scan decks list everything that is moving. This roadmap is deliberately the opposite: each stakeholder chapter includes a short "What you do not need to worry about in 2026-2027" box so you can see, in black and white, which noisy acronyms you can park until after 2027.



EXECUTIVE DASHBOARD

This section is designed to work as a stand-alone board pack page: you can lift the heat map, matrix and timeline directly into ExCo or Board materials. Use it as the anchor slide for any 2026-2027 payments regulation discussion, alongside HM Treasury's Payments Forward Plan for the wider 2026-2028 context.

1. Regulatory Change Heat Maps

Five regulatory changes will reshape the UK and EU payments ecosystem in the next 18 months: UK Safeguarding (CASS 15), UK BNPL Regulation, PSD3 & PSR Adoption, UK Crypto Gateway, and EU AML Regulation (AMLR). This heat map prioritises them by urgency and impact, moving from the imminent (red alert) to the distant but material (green watch). The colours are your signal: red demands action now; amber requires planning; green warrants monitoring. Not every regulation affects every firm, but every firm needs to know which ones do. Start here to find your priorities.

Use this heat map together with the "Most relevant for" lines and the Stakeholder Impact Matrix on the next pages to identify which changes actually apply to your firm and where to find the detailed chapter guidance.

IMPACT / TIMEFRAME	NEAR-TERM (0-6 months)	MEDIUM-TERM (6-18 months)	LONG-TERM (18+ months)
HIGH IMPACT	UK Safeguarding (CASS 15) - 7 May 2026 UK BNPL Regulation - 15 July 2026	PSD3 & PSR Adoption - Q2 2026 / Q4 2027 UK Crypto Gateway Opens - 30 September 2026	EU AML Regulation - 10 July 2027 UK Crypto Regime Live - 25 October 2027
MEDIUM IMPACT	APP Fraud Review - Q3 2026 [10] [11] UK Money Laundering Regulations (MLRs) - 2024 Amendments - Q1 2026	National Payments Vision Implementation	Post-Quantum Cryptography Standards
LOW IMPACT	Critical Third Party (CTP) Designations Begin	EU AI Act - December 2027	Post-Quantum Cryptography Migration Timeline - 2028+ DORA Evolution - 2027-2028 Open Finance Framework Development - 2027-2028

The sections below detail which firms are affected by what.

HIGH IMPACT Changes

Near-term (0-6 months)

REGULATORY REQUIREMENT	WHAT TO EXPECT
UK Safeguarding (CASS 15) - 7 May 2026	• **Applies to**: Authorised PIs, EMIs • **Action**: Implement daily reconciliation, external audit, resolution pack • Most relevant for: PIs & EMIs (Chapter 1) and Safeguarding (Chapter 2)
UK BNPL Regulation - 15 July 2026	• **Applies to**: Third-party BNPL lenders • **Action**: FCA authorisation, creditworthiness frameworks • **Most relevant for**: BNPL Providers (Chapter 5)

Medium-term (6-18 months)

REGULATORY REQUIREMENT	WHAT TO EXPECT
PSD3/PSR Adoption (formal adoption and publication expected during 2026, with first obligations likely to bite from late 2027 after an estimated 18-21 month transition period.)	• **Applies to**: All payment service providers (PSPs) in EU • **Action**: Gap analysis, system readiness (21-month transition period) • **Most relevant for**: Most relevant for: PIs & EMIs (Chapter 1), Safeguarding (Chapter 2), PISPs & AISPs (Chapter 3), Acquirers (Chapter 6), Banks (Chapter 7) and Card Issuers (Chapter 8) with EU operations (alongside the Instant Payments Regulation[12] VoP[13] obligations from 9 October 2025 for credit transfers).
UK Crypto Gateway Opens - 30 September 2026	• **Applies to**: Cryptoasset service providers, stablecoin issuers • **Action**: Application preparation, submit before 28 February 2027 • **Most relevant for**: Cryptoasset Firms (Chapter 4)

Long-term (18+ months)

REGULATORY REQUIREMENT	WHAT TO EXPECT
EU AML Regulation - 10 July 2027	• **Applies to**: All EU-operating financial institutions • **Action**: Monitor AMLA guidance, prepare for direct supervision • **Most relevant for**: EU-facing firms in PIs & EMIs (Chapter 1), Safeguarding (Chapter 2), PISPs & AISPs (Chapter 3), Cryptoasset Firms (Chapter 4), Acquirers (Chapter 6), Banks (Chapter 7) and Card Issuers (Chapter 8)
UK Crypto Regime Live - 25 October 2027	• **Applies to**: All crypto firms serving UK customers • **Action**: Full authorisation required • **Most relevant for**: Cryptoasset Firms (Chapter 4)

MEDIUM IMPACT Changes

Near-term

REGULATORY REQUIREMENT	WHAT TO EXPECT
APP Fraud Review - Q3 2026	• **Applies to**: Faster Payments participants • **Action**: Monitor PSR review outcomes • **Most relevant for**: All in-scope PSPs in Faster Payments and CHAPS (primarily Banks in Chapter 7, plus any PIs/EMIs in Chapter 1 that provide relevant accounts)
UK Money Laundering Regulations (MLRs) - 2024 Amendments - Q1 2026	• **Applies to**: All UK financial institutions (PIs, EMIs, banks, crypto firms, BNPL providers) • **Action**: Review amended AML/CFT obligations; update compliance policies and procedures (21 days post-laying) • **Most relevant for**: UK-facing firms in PIs & EMIs (Chapter 1), Safeguarding (Chapter 2), PISPs & AISPs (Chapter 3), Cryptoasset Firms (Chapter 4), BNPL Providers (Chapter 5), Banks (Chapter 7) and Card Issuers (Chapter 8)

Medium-term

REGULATORY REQUIREMENT	WHAT TO EXPECT
National Payments Vision Implementation	• **Applies to**: Major PSPs, infrastructure providers • **Action**: Engage with Pay.UK forward plan consultation • **Most relevant for**: Larger UK PSPs in PIs & EMIs (Chapter 1), Safeguarding (Chapter 2), Acquirers (Chapter 6) and Banks (Chapter 7)

Long-term (18+ months)

REGULATORY REQUIREMENT	WHAT TO EXPECT
Post-Quantum Cryptography Standards	• **Applies to**: All PSPs with cryptographic systems • **Action**: Assess migration roadmap • **Most relevant for**: Technology and security teams across all stakeholder chapters with significant payments infrastructure

LOW IMPACT Changes

Near-term

REGULATORY REQUIREMENT	WHAT TO EXPECT
Critical Third Party (CTP) Designations Begin (PS16/24[14])	• **Applies to**: Systemically important third-party providers (cloud, data, AI/ML) serving UK financial institutions • **Action**: If designated, comply with FCA/PRA/BoE Fundamental Rules and Operational Risk & Resilience Requirements • **Most relevant for**: Designated CTPs and the largest firms in Acquirers (Chapter 6), Banks (Chapter 7) and Card Issuers (Chapter 8) that rely heavily on them

Medium-term

REGULATORY REQUIREMENT	WHAT TO EXPECT
EU AI Act - December 2027	• **Applies to**: High-risk AI system deployers • **Action**: Monitor EBA guidance on AI in financial services • **Most relevant for**: EU-facing firms in PISPs & AISPs (Chapter 3), Cryptoasset Firms (Chapter 4), Banks (Chapter 7) and Card Issuers (Chapter 8) using high-risk AI for credit, fraud or AML

Long-term (18+ months)

REGULATORY REQUIREMENT	WHAT TO EXPECT
Post-Quantum Cryptography Migration Timeline - 2028+	• **Applies to**: All PSPs with cryptographic systems • **Action**: Begin assessment of migration roadmap; monitor NIST standards implementation guidance • **Most relevant for**: Technology and security teams across all stakeholder chapters
Digital Operational Resilience Act (DORA) Evolution - 2027-2028	• **Applies to**: EU-operating firms with significant ICT dependencies • **Action**: Monitor refinements to third-party monitoring and ICT risk management requirements • **Most relevant for**: EU-facing firms in PIs & EMIs (Chapter 1), Safeguarding (Chapter 2), PISPs & AISPs (Chapter 3), Acquirers (Chapter 6) and Banks (Chapter 7) with material ICT dependencies
Open Finance Framework Development - 2027-2028	• **Applies to**: Payment service providers and account servicing entities • **Action**: Monitor UK and EU guidance on voluntary open finance frameworks beyond PSD3 scope • **Most relevant for**: ASPSPs and data-rich providers in PIs & EMIs (Chapter 1), Safeguarding (Chapter 2), PISPs & AISPs (Chapter 3) and Banks (Chapter 7)

2. Stakeholder Impact Matrix

The heat maps told you what's urgent. This matrix tells you what's yours. While the regulatory heat map ranks by alarm level, the impact matrix serves as your compliance inventory: a quick guide mapping every key regulation across eight stakeholder types. Not everything here demands action; some duties are ongoing. But everything applies to someone. The question is whether it applies to you.

The matrix uses principle-based logic across UK and EU frameworks. For jurisdiction-specific or business-model nuances, see the detailed guidance sections. If your group plays more than one role (for example PI + acquirer, or bank + BNPL), read down all relevant columns when building your compliance inventory.

Legend:

✅ Directly impacted: mandatory compliance required in principle

⚠️ Conditionally impacted: application depends on specific business model, geography, or service type; see stakeholder chapter for details

❌ Not directly impacted or out of scope by regulatory principle or covered under other regulations

Regulatory Change	PIs	EMIs	Banks	Acquirers	Issuers	PISP/ AISP	Crypto Firms	BNPL Providers
UK Safeguarding (CASS 15)	✅	✅	❌	⚠️	❌	⚠️	❌	❌
EU E-Money Safeguarding (EMD2 / PSD3)	⚠️	✅	❌	⚠️	❌	⚠️	❌	❌
UK Confirmation of Payee (CoP)	✅	✅	✅	⚠️	✅	⚠️	❌	❌
EU Verification of Payee (VoP)	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	❌	❌
UK APP Fraud Reimbursement	✅	✅	✅	⚠️	✅	⚠️	❌	❌
EU PSD3 Fraud Prevention & Spoofing Liability	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	❌	❌
EU PSD3 Open Banking Access	✅	⚠️	⚠️	❌	❌	✅	❌	❌
UK Crypto Authorisation (FSMA 2023)	⚠️	⚠️	⚠️	❌	❌	❌	✅	❌
EU Cryptoasset Regulation (MiCAR)	⚠️	⚠️	⚠️	❌	❌	❌	✅	❌
UK BNPL Regulation	❌	❌	❌	❌	⚠️	❌	❌	✅
EU BNPL Regulation	❌	❌	❌	❌	⚠️	❌	❌	⚠️
UK Money Laundering Regulations (MLRs) 2024 Amendments	✅	✅	✅	✅	✅	✅	✅	✅
EU Anti-Money Laundering Regulation (AMLR)	✅	✅	✅	✅	✅	✅	✅	✅
UK/EU Operational Resilience	⚠️	⚠️	✅	⚠️	⚠️	⚠️	⚠️	⚠️
UK Critical Third Party (CTP) Designations	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️
UK/EU AI Governance & Explainability	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	✅	⚠️
UK/EU Post-Quantum Cryptography Standards	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️

3. Critical Milestone Timeline

This is your regulatory implementation calendar for 2026-2027. Consider this your payments industry calendar of pain, colour-coded by severity. Some dates are hard stops (red); others require active planning (amber); the rest warrant monitoring (green). Bookmark this section. Your CFO will thank you.

Q1 2026	🟡 UK MLR amendments (21 days post-laying) 🟡 BNPL policy statement expected (early Q1) 🟡 PSD3 political agreement reached November 2025; formal adoption and publication expected during 2026 (Council and Parliament texts to be finalised)
Q2 2026	🔴 7 May: UK Safeguarding (CASS 15) effective date 🔴 July: First safeguarding audit submissions (with 6-month grace period) 🟡 July: FCA crypto PASS opens, draft application forms published 🔴 15 July: UK BNPL regulation effective
Q3 2026	🟡 APP fraud reimbursement review (PSR) 🟡 30 September: UK Crypto authorisation gateway opens
Q4 2026	🟡 EU BNPL regulation (20 November) 🟢 FCA AI governance guidance deadline (December) 🟡 PSD3/PSR publication in the Official Journal expected during 2026, followed by national implementation work and development of EBA technical standards
Q1-Q2 2027	🟡 Crypto gateway application period continues (closes 28 February) 🟡 PSD3 EBA technical standards development
Q3 2027	🔴 10 July: EU AML Regulation effective
Q4 2027	🔴 25 October: UK Crypto regime go-live 🟡 PSD3/PSR application expected from late 2027 into 2028, following an estimated 18-21 month transition period after 2026 adoption 🟢 EU AI Act application begins (December)

This executive dashboard gives you the panoramic view. The sections that follow zoom in on your specific corner of the payments ecosystem. Whether you operate payment institutions, issue e-money, acquire on behalf of merchants, deploy AI, or offer buy-now-pay-later credit, the chapters below map precisely which regulations apply to you, which don't, and what you need to do by when.

Start with your stakeholder type. Read the heat map items that affect you. Then follow the implementation roadmap for your firm size and business model. Confusion about regulatory scope ends here, and everything on these pages can be lifted directly into your internal regulatory roadmap pack.

As you move from the Dashboard into your stakeholder chapters, use the “What you do not need to worry about in 2026-2027” sections as deliberate brakes: they are there to stop you burning budget on regimes that are background noise for your business model this side of 2028.

Chapter 1: Payment Institutions & E-Money Institutions

If you're a PI or EMI, congratulations: you're regulated on both sides of the Channel, and the rules are different. This chapter maps what applies to you in the UK versus the EU, where the EU is moving towards a single, harmonised PSD3/PSR regime for payment and e-money institutions, while the UK is introducing a distinct CASS 15 trust-based safeguarding framework with no direct EU equivalent.

It stays focused on who is in scope, what they must do, and when, covering authorised PIs and EMIs in the UK and EU plus Small EMIs and SPIs that opt in to safeguarding. Detailed safeguarding requirements are covered in Chapter 2, and PISPs and AISPs are addressed in later chapters.

For clarity, the analysis here does not cover BNPL regimes (see later section), bank prudential rules (CRD IV/CRR), or individual card-scheme rulebooks, except where explicitly flagged.



1.1 Regulatory Requirements: PIs vs EMIs (Consolidated Table)

The table below provides an overview of key regulatory requirements by geography and entity type. Detailed safeguarding requirements are covered in Chapter 2.

Legend: ✅ Applies / Mandatory ⚠️ Limited / Principles-based guidance ❌ Does not apply / No obligation

REGULATORY REQUIREMENT	UK-OPERATING PIs	EU-OPERATING PIs	UK-OPERATING EMIs	EU-OPERATING EMIs
UK: Safeguarding (CASS 15) FCA PS25/12	✅ Mandatory (if UK-authorised, holding relevant funds)	❌ Not applicable	✅ Mandatory (if UK-authorised, holding e-money; 100% of e-money issued)	❌ Not applicable
UK: Confirmation of Payee (CoP) PSR SD17	✅ Mandatory (if Faster Payments/CHAPS participant, since October 2024)	❌ Not applicable	✅ Mandatory (if Faster Payments/CHAPS participant, since October 2024)	❌ Not applicable
UK: Operational resilience FCA/PRA/BoE PS21/3	✅ Mandatory (UK-specific requirements)	❌ Not applicable	✅ Mandatory (UK-specific requirements)	❌ Not applicable
UK: APP fraud reimbursement PSR SD20 (FPS) & SD21 (CHAPS)	✅ Mandatory (if FPS or CHAPS direct/indirect participant, since 7 October 2024)	❌ Not applicable	✅ Mandatory (if FPS or CHAPS direct/indirect participant, since 7 October 2024)	❌ Not applicable
UK: Crypto authorisation FSMA 2023	✅ Mandatory (if offering crypto-related payment services to UK customers)	❌ Not applicable	✅ Mandatory (if issuing stablecoins or offering crypto services to UK customers)	❌ Not applicable
EU: Verification of Payee (VoP) Regulation 2024/886	❌ Not applicable	✅ Mandatory (if executing credit transfers, from 9 October 2025)	❌ Not applicable	✅ Mandatory (if executing credit transfers, from 9 October 2025)
EU: PSD3 fraud & consumer protection	❌ Not applicable	✅ Mandatory (spoofing liability, enhanced SCA, fraud prevention; application from late 2027 after an 18-21 month transition)	❌ Not applicable	✅ Mandatory (same as for PIs)
EU: EMD2 (current e-money safeguarding)	❌ Not applicable	❌ Not applicable (PIs under PSD2, not EMD2)	❌ Not applicable	✅ Mandatory (safeguarding of 100% of e-money issued)
EU: PSD3/PSR (merger of PI and EMI regimes, repeals EMD2)	❌ Not applicable	✅ Mandatory after 2026 adoption and an 18-21 month transition, with first obligations from late 2027; PIs will be able to issue e-money under a single framework	❌ Not applicable	✅ Mandatory once PSD3/PSR applies after 2026 adoption and an 18-21 month transition, with PI and EMI regimes merged and EMD2 repealed
EU: Operational resilience (PSD2 Articles 95-96, transitioning to PSD3)	❌ Not applicable	✅ Mandatory (incident reporting and security measures)	❌ Not applicable	✅ Mandatory (will move into PSD3/PSR framework)

Note: Firms operating in both the UK and EU must comply with all applicable requirements in each jurisdiction. EU EMIs are currently subject to EMD2 safeguarding and will move to the harmonised PSD3/PSR framework once it applies after the transition period.

1.2 Priority Action Timeline: PIs & EMIs (UK & EU)

If you are UK-only, focus on the UK-operating PIs and EMIs column; if you have EU entities or branches, you must work through both UK and EU timelines in parallel. This timeline highlights new or intensified change activity for 2026-2027. It assumes that ongoing obligations already in force (for example existing APP fraud reimbursement and Confirmation of Payee/Verification of Payee where applicable) are being met as business-as-usual and only reappear here if there is a specific new milestone or review.

UK-Operating PIs and EMIs	EU-Operating PIs and EMIs
🔴 **IMMEDIATE (by 7 May 2026): UK Safeguarding Implementation** Implement CASS 15 safeguarding (daily reconciliation, audit, resolution pack, SMCR ownership) - see Chapter 2 sections 2.2.3 and 2.2.4 for detailed requirements and timelines.	🟡 **Q2-Q3 2026: PSD3 Gap Analysis** Conduct PSD3/PSR gap analysis, including VoP, fraud liability and safeguarding changes - see Chapter 2 section 2.3 and 2.4 for detailed EU requirements.
All PIs and EMIs (UK and EU)	
🟡 **Q3-Q4 2026: Operational & Compliance** • Review operational resilience incident reporting readiness • Where crypto services are offered, prepare any required UK authorisation application aligned with FSMA 2023. • Monitor APP fraud reimbursement developments and PSR consultations. For EU operations executing credit transfers, confirm that Verification of Payee (VoP) implementation remains compliant with Instant Payments Regulation timelines and any local supervisory guidance. 🟢 **2027: Long-term Planning** • Implement PSD3/PSR changes during the expected transition window (around 18-21 months post-adoption). • For EU operations, prepare for EU AML Regulation application from 10 July 2027. • Continue to build AI governance frameworks for fraud detection and transaction monitoring.	

1.3 Building your PI/EMI roadmap (UK & EU

Implementing CASS 15, preparing for PSD3/PSR, and adapting to new fraud and operational resilience expectations will require coordinated change across compliance, finance, operations, and technology. Rather than treating these as isolated projects, firms should build a multi-year regulatory change roadmap that covers both UK and EU obligations where relevant.

Firms should assess implementation resource needs based on factors such as:

- payment volumes and e-money outstanding,
- the number of segregated client and safeguarding accounts and jurisdictions,
- existing reconciliation and reporting infrastructure,
- whether they operate in the UK only, in the EU only, or in both,
- and the availability of in-house compliance, treasury, and technology expertise.

Typical workstreams include gap analysis, system and data changes, external safeguarding, and statutory audit engagement, SMCR governance updates, and ongoing BAU reconciliation, monitoring, and reporting. Firms that start with a realistic view of their capacity, clear ownership, and early engagement with auditors, legal advisers, and key banking partners will be better placed to execute the safeguarding, fraud, and resilience changes set out in this chapter, and to scale their approach as PSD3/PSR and related regimes come into force - ideally because they planned for impact, not because a regulator's letter finally ruined their Friday afternoon.

1.4 What PIs and EMIs do not need to worry about in 2026-2027

1.4.1 BNPL Regulation (Buy Now Pay Later)

Why it doesn't apply to PIs/EMIs	When it DOES apply:
• BNPL is a credit product regulated by the FCA under Consumer Credit framework • PIs/EMIs provide payment services and e-money, not credit • Unless a PI or EMI separately offers BNPL products (e.g. a PI offering both payment accounts and BNPL credit lines), they are out of scope	• If your PI/EMI subsidiary or division separately offers BNPL products • If your PI/EMI partners with BNPL providers and directly facilitates credit offerings

1.4.2 CRD IV/CRR Prudential Regime

Why it doesn't apply to PIs/EMIs	When it DOES apply:
• CRD IV (Capital Requirements Directive IV) and CRR (Capital Requirements Regulation) apply to banks and investment firms • PIs and EMIs operate under separate capital regimes: – PIs: Capital requirements under PSRs 2017 (Risk Weighting Model or Fixed Percentage Model) – EMIs: Capital requirements under EMRs 2011 (2% of average outstanding e-money or Fixed Percentage Model) • These regimes are simpler and less onerous than CRD IV/CRR	• If your PI/EMI plans to become a bank.

1.4.3 Card Scheme Rules (Visa/Mastercard)

Why it doesn't apply to PIs/EMIs	When it DOES apply:
• Card scheme rules apply only to scheme members (issuers, acquirers) • PIs and EMIs may not hold scheme membership	• If your PI/EMI operates as a card acquirer (processes merchant card transactions). • If your PI/EMI issues branded payment cards (operates as a card issuer for a given card scheme). • If your PI/EMI holds membership of Visa, Mastercard, or other schemes.

Chapter 2: Safeguarding Requirements for PIs & EMIs

This chapter consolidates safeguarding obligations for Payment Institutions and E-Money Institutions across UK and EU jurisdictions. Safeguarding is the foundational customer protection mechanism: the requirement to segregate and protect customer funds (relevant funds and e-money) held by payment service providers.

Stakeholders covered:

- UK-authorised Payment Institutions (holding relevant funds)
- UK-authorised E-Money Institutions (issuing e-money)
- EU-authorised Payment Institutions
- EU-authorised E-Money Institutions

2.1 Safeguarding Requirements Comparison Tables

Use the tables in this section for a quick overview of the principles and requirements.

2.1.1 Generic principles

Dimension	UK CASS 15 (Effective 7 May 2026)	EU EMD2/PSD2 (current)	EU PSD3/PSR (post-2027)
Prescriptiveness	**High** (prescriptive rules)	**Medium** (principles-based)	**High** (expected, pending standards)
Operational burden	**High** (daily reconciliation, audit, resolution pack)	**Medium** (ongoing 100% safeguarding only)	**High** (expected, pending standards)
Immediate compliance deadline	**7 May 2026**	**Ongoing** (current regime)	**Around 2027-2028** (following adoption and transition period).
Strategic opportunity	Plan for post-PSD3 central bank access	Prepare for PSD3 transition	Assess and, where appropriate, leverage central bank access.

Key observations

1. UK CASS 15 (effective May 2026) is significantly more prescriptive than current EU regimes (daily reconciliation, annual audit, SMCR accountability).
2. EU EMD2 and PSD2 are principles-based, with less granular operational requirements.
3. PSD3/PSR (from late 2027 into 2028) will narrow the gap by introducing a single regime for PIs and EMIs and adding tools such as diversification and optional central bank accounts, but details depend on final EBA technical standards.
4. Optional central bank access, where available, could be structurally significant for the post-2027 safeguarding landscape in the EU, especially for larger institutions.
5. Harmonisation risk: UK may diverge from EU post-2027 as implementation details finalised (regulatory fragmentation).

2.1.2 PIs and EMIs: UK vs. EU requirements (current and near-term)

Legend: ✅ Applies/ Mandatory ⚠️ Limited / Principles-based guidance ❌ Doesn't apply/ No obligation

REQUIREMENT	UK PIs (CASS 15)	UK EMIs (CASS 15)	EU PIs (PSD2 current)	EU EMIs (EMD2 current)	EU PIs/EMIs (PSD3/PSR post-2027)
Funds to be safeguarded	100% of relevant funds (not immediately transmitted)	100% of e-money issued	100% of relevant funds (not immediately transmitted)	100% of e-money issued	100% of relevant funds and e-money under a single PI licence (merged framework)
Safeguarding methods	Segregation, liquid assets, or insurance	Segregation, liquid assets, or insurance	Segregation, liquid assets, or insurance	Segregation, liquid assets, or insurance	Segregation, liquid assets, insurance, and, where available, central bank deposits
Daily reconciliation	✅ Mandatory	✅ Mandatory	❌ Not required (principles-based)	❌ Not required (principles-based)	✅ Likely enhanced reconciliation frequency (details via EBA standards TBD)
Annual audit	✅ Mandatory (over £100k threshold)	✅ Mandatory (over £100k threshold)	❌ Not mandatory (EBA guidance only)	❌ Not mandatory (EBA guidance only)	✅ Audit and assurance expectations likely to increase (national rules and EBA standards TBD)
Due diligence on safeguarding banks	✅ Mandatory, ongoing	✅ Mandatory, ongoing	✅ Mandatory, ongoing	✅ Mandatory, ongoing	✅ Mandatory, ongoing
Insurance/guarantee conditions	✅ No payout restrictions allowed	✅ No payout restrictions allowed	⚠️ Principles-based (no specific restrictions mandated)	⚠️ Principles-based (no specific restrictions mandated)	✅ Expected (EBA standards TBD)
Resolution pack	✅ Mandatory	✅ Mandatory	❌ Not explicitly required (good practice)	❌ Not explicitly required (good practice)	✅ Wind-down / winding-up planning required; resolution-pack-style documentation likely in practice
SMCR Senior Manager designation	✅ Mandatory (UK-specific regime)	✅ Mandatory (UK-specific regime)	❌ Not applicable (EU governance rules differ)	❌ Not applicable (EU governance rules differ)	❌ Not applicable (EU applies its own management body and governance regime)
Central bank safeguarding access	❌ Not currently available	❌ Not currently available	❌ Not currently available	❌ Not currently available	⚠️ Optional, subject to central bank discretion (post-2027)
Effective date	7 May 2026	7 May 2026	Current (ongoing)	Current (ongoing)	Application expected from late 2027 into 2028 (after formal adoption during 2026 and an estimated 18-21 month transition period)

2.2 UK Safeguarding (CASS 15)

Effective Date: 7 May 2026

Background:

UK safeguarding reforms (Client Assets Sourcebook - CASS 15) respond to failures where firms held insufficient or poorly recorded customer funds, causing delays and losses. They make safeguarding clearer, more consistent and robust, aligning payment and e-money safeguarding more closely with the investment firm client money regime (CASS 7).

Applies to:

- Authorised Payment Institutions (PSRs 2017, Regulation 19)
- Authorised E-Money Institutions (EMRs 2011, Regulation 20)
- Small E-Money Institutions (EMRs 2011)
- Credit unions issuing e-money

2.2.1 What PIs Must Safeguard (UK)

RELEVANT FUNDS	• Customer funds received for execution of payment transactions. • Funds held pending execution of payment orders. • Funds received from payment service users to provide payment services • PIs must safeguard 100% of relevant funds
SAFEGUARDING METHODS (any one or combination)	• Segregation in dedicated safeguarding accounts at authorised credit institutions. • Investment in secure, liquid assets that meet FCA conditions for safeguarding. • Insurance policy or comparable guarantee covering safeguarded amounts.
NOT SAFEGUARDED	• Firm's own working capital. • Funds immediately executed (no holding period). • Collateral or security deposits.

2.2.2 What EMIs Must Safeguard (UK)

At the risk of teaching grandmother to suck eggs, here's a quick definition...

E-money is an electronic store of monetary value that is issued on receipt of funds, accepted as means of payments by third parties other than the issuer and is redeemable at par value. So, what are the safeguarding obligations for EMIs?

E-MONEY	• 100% of outstanding e-money value must be safeguarded at all times. • Calculated daily, reconciled daily under CASS 15. • Higher materiality than payment institutions (often larger balances).
SAFEGUARDING METHODS (any one or combination)	• Segregation in dedicated safeguarding accounts at authorised credit institutions. • Investment in secure, liquid assets that meet FCA conditions for safeguarding. • Insurance policy or comparable guarantee covering the full safeguarded amount.
NOT SAFEGUARDED	• Firm's own working capital. • Fees and charges already earned by the EMI, once clearly separated from customer e-money. • Funds immediately executed (no holding period) • Any funds the firm holds that do not represent issued e-money (for example, funds received for other services, appropriately distinguished in the firm's records). • Collateral or security deposits.

Example: If an EMI has £10 million in customer e-money balances, £10 million must be held in segregated safeguarding accounts or covered by insurance/guarantee.

2.2.3 CASS 15 Core Requirements (UK)

CASS 15 is the FCA's seven-step safeguarding routine: the steps are the same for everyone; the pain depends on your size and how tidy your books already were. The table below strips each step back to what it actually requires and where it bites operationally.

#	REQUIREMENT	WHAT IT MEANS	IMPACT
1	**Daily Reconciliation (MANDATORY)**	• Safeguarded funds must be reconciled on each reconciliation day (in practice every business day, excluding weekends and relevant bank holidays). • Internal reconciliation: Compare requirements (what should be held) vs. resources (what is held). • External reconciliation: Confirm balances with safeguarding banks/custodians. • Non-standard reconciliation methods require independent auditor's report and disclosure in monthly returns.	**Operational impact:** • End of monthly/weekly reconciliation is replaced by daily process. • Real-time or near-real-time safeguarding calculations required. • Systems must produce accurate, granular data at each reconciliation point.
2	**Annual Safeguarding Audit (MANDATORY for most firms)**	• External audit of safeguarding arrangements by qualified, regulated auditor. • Audit must cover: accuracy of books and records, effectiveness of internal safeguarding systems and controls. • Exception: if firm did not safeguard over £100,000 of relevant funds at any point in previous 53 weeks, audit not required.	**Grace period:** • The first safeguarding audit must be submitted within 6 months of the end of the first period after 7 May 2026; subsequent audits are expected within 4 months of period end. **What auditors will examine:** • Reconciliation processes and documentation. • Segregation of safeguarded funds from firm's own funds. • Due diligence on safeguarding banks. • Resolution pack adequacy. • Governance and oversight (SMCR Senior Manager designation).
3	**Due Diligence on Third Parties (MANDATORY)**	• Conduct due diligence at appointment of safeguarding banks/custodians. • Periodic due diligence thereafter. • Assess creditworthiness, financial stability, operational resilience. • Document due diligence process and findings.	**Operational implication:** • Cannot simply use any bank: must actively assess suitability. • Ongoing monitoring obligation (not just one-time check). • Documented evidence required for auditors.
4	**Insurance/Guarantee Conditions** (if using insurance method)	• Safeguarding insurance policies or comparable guarantees must not include restrictions on payout except for confirming an insolvency event. • Policy must cover full amount of safeguarded funds. • Contingency planning: At least 3 months before policy expires, firm must have plan for renewal or alternative safeguarding.	**Compliance implication:** • "Claims-made" policies with extensive exclusions likely non-compliant. • Must be able to access insurance proceeds quickly in insolvency. • No "gap" periods without coverage.

#	REQUIREMENT	WHAT IT MEANS	IMPACT
5	**Diversification (BEST PRACTICE,** supervisory expectation)	**Guidance:** • Firms should not hold all safeguarded funds with a single safeguarding bank. • Diversification reduces counterparty risk (if a safeguarding bank fails, not all customer funds are exposed). • While not yet a hard rule, the FCA increasingly expects meaningful diversification, particularly for larger firms.	**Operational implication:** • Requires firms to maintain multiple safeguarding banks or methods, especially as balances grow. • Drives additional treasury, legal and operational work (onboarding extra banks, updating agreements, adjusting reconciliations). • Increases resilience to single-bank failure but can add complexity to daily reconciliation and liquidity management.
6	**Resolution Pack (MANDATORY)**	• Prepare and maintain comprehensive documentation for use in failure scenario. • Must enable insolvency practitioner to quickly identify and return safeguarded funds.	**Resolution pack contents:** • Locations of safeguarded funds (account details, balances). • Details of agents and distributors (if funds held via intermediaries). • Flow of funds diagrams (how money moves through business). • Customer data (who is owed what). • Reconciliation methodologies. • Contact details for safeguarding banks and key personnel. **Operational implication:** • Cannot be assembled during failure: must be maintained continuously. • Must be accessible to insolvency practitioner (not just compliance team). • Test the pack: can external auditor understand it?
7	**SMCR Senior Manager Designation (MANDATORY)**	• Designated Senior Manager under Senior Managers & Certification Regime responsible for safeguarding. • In practice, SMF16 (Compliance Oversight) or SMF17 (Money Laundering Reporting Officer) is often designated, but firms should confirm the most appropriate role for their governance structure. • Personal accountability for safeguarding framework effectiveness.	• Elevates safeguarding from a "back-office process" to a board-visible accountability with a named Senior Manager. • Requires clear documentation of roles, responsibilities and MI for safeguarding across compliance, finance, treasury and operations. • Increases the personal regulatory risk for the designated SMF holder, which in turn tends to drive stronger challenge, escalation and investment in safeguarding controls.

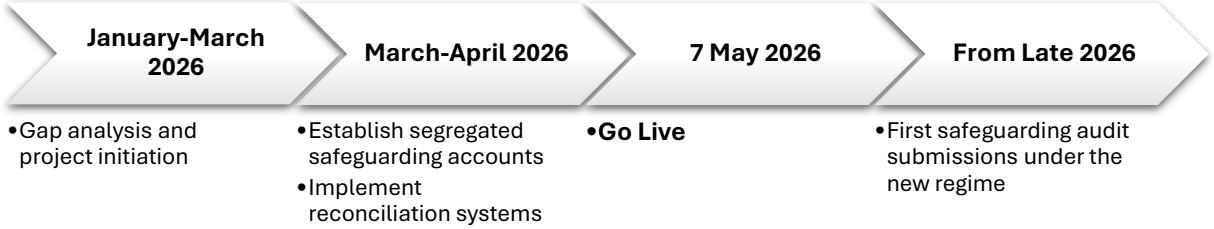
2.2.4 Implementation Timeline (UK CASS 15)

By 7 May 2026, firms must:

- Implement daily internal and external reconciliation processes.
- Engage qualified, regulated auditor for annual safeguarding audit.
- Conduct due diligence on all safeguarding banks/custodians.
- If using insurance: Review policy terms, ensure no payout restrictions, establish 3-month contingency window.
- Create and test resolution pack.
- Designate SMCR Senior Manager for safeguarding oversight.
- Update internal policies and procedures to reflect CASS 15 requirements.
- Train relevant staff on new requirements and operational changes.
- Establish monitoring framework for ongoing compliance.

- Prepare for the first safeguarding audit submission within 6 months of the end of the first reporting period after 7 May 2026, and within 4 months for subsequent periods.

Project timeline:



2.3 EU E-Money Safeguarding (EMD2 & PSD3 Transition)

Current regime: Electronic Money Directive 2 (EMD2)

Transition regime: PSD3/PSR (estimated Q4 2027 implementation)

Applies to:

- EU-authorised E-Money Institutions (under EMD2, current regime).
- EU-authorised Payment Institutions (under PSD2, current regime; future PSD3/PSR regime).
- Both stakeholder types will transition to harmonised PSD3/PSR framework.

2.3.1 Current EU E-Money Safeguarding (EMD2 - pre-PSD3)

E-MONEY	• 100% of outstanding e-money value must be safeguarded at all times.
SAFEGUARDING METHODS (any one or combination)	• Segregated accounts at authorised credit institutions in EU (or with central bank if permitted). • Liquid assets (government securities, high-grade corporate bonds) in dedicated accounts. • Insurance policy covering full e-money value issued.
DUE DILIGENCE ON SAFEGUARDING BANKS	• EMIs must conduct due diligence on credit institutions holding segregated funds. • Ongoing monitoring obligation. • Assessment of credit institution's creditworthiness and operational stability.
NOT SAFEGUARDED	• Firm's own working capital. • Fees and charges already earned by the EMI, once clearly separated from customer e-money. • Funds immediately executed (no holding period) • Any funds the firm holds that do not represent issued e-money (for example, funds received for other services, appropriately distinguished in the firm's records). • Collateral or security deposits.

Key difference from UK CASS 15:

- No prescriptive daily reconciliation requirement.
- No mandatory annual audit requirement (though EBA guidance recommends assurance).
- Less granular operational oversight than CASS 15.

2.3.2 EU Payment Institution Safeguarding (PSD2 - pre-PSD3)

RELEVANT FUNDS	• Customer funds received for execution of payment transactions. • Funds held pending execution of payment orders. • Funds received from payment service users to provide payment services • PIs must safeguard 100% of relevant funds
SAFEGUARDING METHODS (any one or combination)	• Segregation in dedicated safeguarding accounts at authorised credit institutions. • Investment in secure, liquid assets that meet PSD2 conditions for safeguarding. • Insurance policy or comparable guarantee covering safeguarded amounts.
NOT SAFEGUARDED	• Firm's own working capital. • Funds immediately executed (no holding period). • Collateral or security deposits.

Key differences from EMIs:

- PIs benefit from similar exemptions to the UK (for example, funds immediately transmitted or held for other PSPs), but the detail is set at national level and in EBA guidance.
- Less prescriptive than EMD2 (no mandatory audit, no daily reconciliation).
- Relies more on principles-based guidance from EBA.

2.3.3 PSD3/PSR Safeguarding Framework (Post-Q4 2027)

Structural change:

- PSD3/PSR will merge Payment Institutions and E-Money Institution regimes into single unified framework.
- EMD2 will be repealed.
- Safeguarding provisions will be harmonised across both stakeholder types.

Expected PSD3/PSR safeguarding requirements (estimated, based on current proposal)

SAFEGUARDED FUNDS	• Continued requirement to safeguard 100% of customer funds and e-money, with methods set out in PSD3/PSR and detailed in EBA technical standards. • An additional option to safeguard client funds in accounts at national central banks, at the discretion of each central bank.
NEW OBLIGATION	• Manage concentration risk, including diversification of safeguarding methods and limits on reliance on a single institution.
OTHER	• EBA-developed regulatory technical standards on safeguarding risk management, which are likely to increase the level of operational detail on reconciliation, governance, and oversight (but may not mirror CASS 15). • Due diligence and notification requirements in relation to safeguarding arrangements to be specified in PSD3/PSR and EBA standards.

Strategic impact:

- Reduced dependence on commercial banks for safeguarding, for firms that can access central bank accounts.
- Potential deposit outflow from commercial banks (safeguarded funds moved to central banks).
- Enhanced customer protection (central bank = lowest credit risk).
- Closer alignment in overall outcomes with the UK (stronger customer money protection), but via a different legal and operational architecture.

2.3.4 Central Bank Safeguarding Access (PSD3 Opportunity)

PSD3 provision (EU only):

- Payment institutions and e-money institutions will be able to safeguard funds directly with central banks under PSD3/PSR where this is permitted.
- This materially reduces safeguarding counterparty risk (central bank versus commercial bank), but any cost impact will depend on each central bank's account terms.
- Central banks are not obliged to offer such accounts; availability and conditions will vary by jurisdiction.

Timeline (EU):

- This option is in the PSD3 proposals, with adoption and publication expected in 2026 and application after an estimated 18-21 month transition, so the first PSD3 safeguarding obligations are likely to bite from late 2027 into 2028, depending on national deployment.

Strategic implications for larger EU PIs/EMIs include:

- A new safeguarding option at central banks.
- Potential reallocation of safeguarded balances away from some commercial banks.
- The need to weigh operational requirements and access criteria at each central bank.

2.4 Priority Actions by Jurisdiction

If you are UK-only, focus on the UK actions in 2.4.1; if you have EU entities or branches, you must plan against both 2.4.1 (UK CASS 15) and 2.4.2 (EU EMD2/PSD3) in parallel.

2.4.1 UK (CASS 15 - Deadline 7 May 2026)

Q1 2026
(Immediate)

- Gap analysis: Compare current safeguarding arrangements to CASS 15 requirements.
- Assess reconciliation systems: Do they support daily internal and external reconciliation?
- Identify safeguarding banks: Document current arrangements, begin due diligence assessment.
- Engage auditor: Identify and brief qualified, regulated auditor on CASS 15 requirements.
- Assess insurance/guarantee: If using insurance method, review policy terms for payout restrictions.

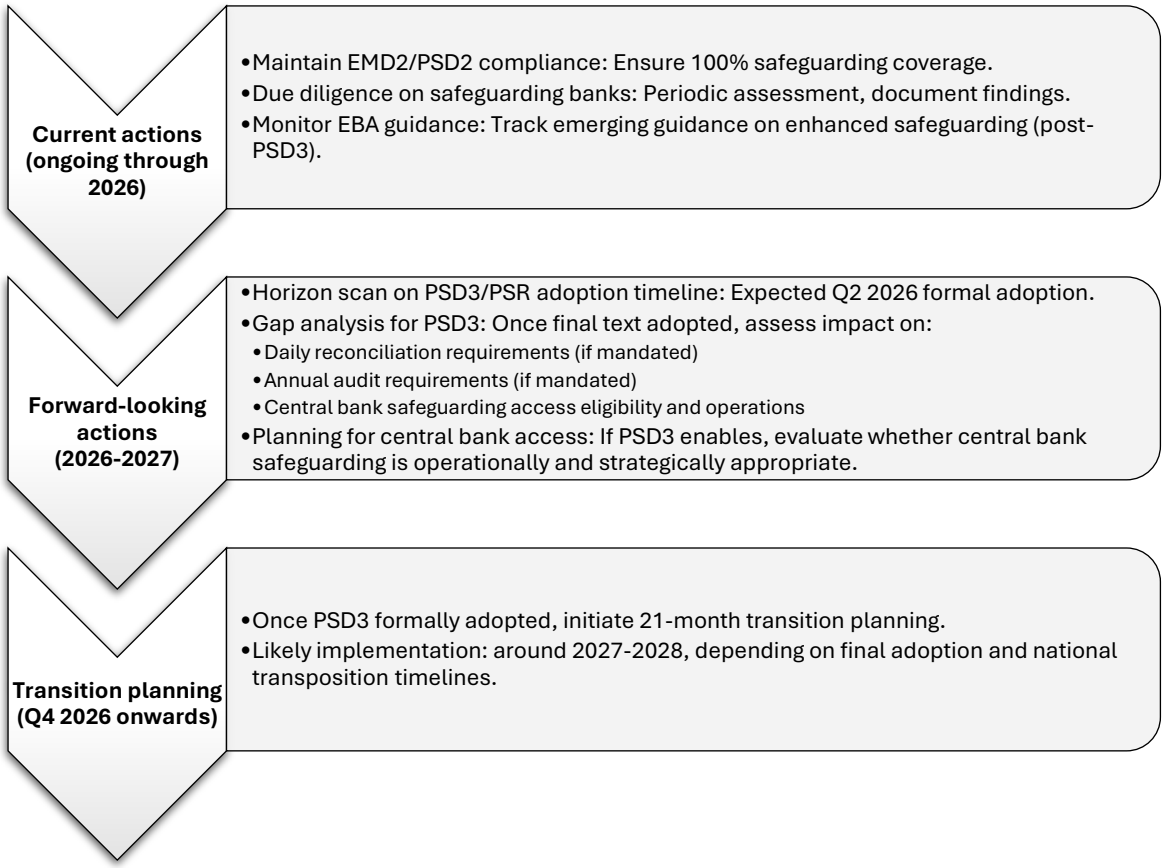
Q1-Q2 2026
(Near term)

- Implement reconciliation systems: Deploy daily reconciliation capability.
- Update policies and procedures: Reflect CASS 15 requirements.
- Conduct staff training: Compliance, operations, finance teams.
- Establish resolution pack: Draft locations, agents, fund flow diagrams.
- Designate SMCR Senior Manager: Notify FCA of designation.

Q2 2026
(Go Live actions)

- **7 May 2026**: CASS 15 effective, safeguarding systems go live.
- From mid-2026: Prepare first safeguarding returns and audit documentation under the new regime.
- Within 6 months of the end of the first reporting period after 7 May 2026: submit the first safeguarding audit, then within 4 months for subsequent periods.

2.4.2 EU (Current EMD2/PSD2 - Monitor for PSD3 Transition)



2.5 Resource Requirements by Firm Size

Implementing CASS 15 and preparing for PSD3/PSR will require various levels of effort depending on firm size, complexity, and the starting maturity of safeguarding arrangements. In other words, every firm has to do the work; what changes with size is not whether you dance, but how big the troupe, how complex the steps, and how long the rehearsal. Firms should use the dimensions below to scope their own resourcing envelope.

2.5.1 Small PIs/EMIs (< £50M annual payment volume)

UK CASS 15 implementation (by 7 May 2026):	EU PSD3/PSR (if EU-authorised)
Focus on a contained project to introduce daily reconciliation, update safeguarding policies and contracts, and put in place audit-ready documentation, with a modest uplift in BAU effort to run reconciliations and respond to audit queries.	Focus on understanding the final PSD3/PSR text, assessing gaps against existing EMD2/PSD2-based processes, and planning incremental changes rather than wholesale system rebuilds.

Typical resourcing pattern:

A safeguarding/compliance lead with support from operations / reconciliation staff, plus external audit and limited advisory input on design and testing.

2.5.2 Medium PIs/EMIs (£50M-£250M annual payment volume)

UK CASS 15 implementation (by 7 May 2026):	EU PSD3/PSR (if EU-authorised)
More structured multi-month work to industrialise safeguarding, including more automated daily reconciliations, clearer SMCR and committee oversight, and fully documented resolution packs.	A defined PSD3/PSR workstream to interpret EBA standards, update safeguarding methods (for example diversification), and align incident, reporting, and governance processes across UK and EU entities where possible.

Typical resourcing pattern:

Compliance and risk leads, a dedicated reconciliation or treasury function, technology and data support, and external legal/audit advisers involved at key design and validation stages.

2.5.3 Large PIs/EMIs (> £250M annual payment volume)

UK CASS 15 implementation (by 7 May 2026):	EU PSD3/PSR (if EU-authorised)
Full regulatory change programme, with project management, technology, treasury, finance, and operations involved to deliver scalable daily reconciliation, MI and audit trails across multiple products and entities.	A cross-functional PSD3/PSR programme that covers safeguarding, fraud, SCA, operational resilience, and potential central bank safeguarding options, coordinated with UK change so firms avoid building two entirely separate regimes.

Typical resourcing pattern:

Dedicated regulatory change team, senior SMCR and board engagement, significant technology and data work, and ongoing engagement with auditors, legal counsel, and key safeguarding banks or central banks.

2.5.4 Resourcing Recap

Across all sizes, the main drivers of resource needs are:

- whether the firm is UK-only, EU-only, or both;
- the complexity of its safeguarding structures (number of banks, currencies, and jurisdictions);
- the maturity of existing reconciliation and governance processes;
- and how far it chooses to go beyond minimum requirements to build a long-term, scalable safeguarding and regulatory compliance model.

Early clarity on those dimensions will help you avoid both under-sourcing (and missing the deadline) and over-sourcing (and burning money on gold-plating).

2.6 Risk Factors & Mitigation

2.6.1 Operational Risks

RISK	MITIGATION
Daily reconciliation systems fail or produce inaccurate data	Implement robust reconciliation platform, test before go-live, establish manual backup procedures, conduct regular system audits.
Safeguarding bank fails or restricts access	Diversify across multiple safeguarding banks, conduct ongoing due diligence, monitor regulatory announcements (FSCS coverage, central bank support).
Insurance policy excludes coverage due to ambiguous terms	Engage specialist insurance broker, ensure policy explicitly covers full safeguarded amount with no payout restrictions, plan for 3-month renewal window.
Inaccurate classification or segregation of funds (customer vs firm funds, relevant funds vs non-relevant funds)	Strengthen data models and chart of accounts, enforce clear account-naming conventions, and run periodic sample reviews to confirm correct classification.

2.6.2 Regulatory Risks

RISK	MITIGATION
FCA enforcement action for non-compliance	Implement compliant systems by 7 May 2026, engage external auditor early, document all design decisions and testing.
CASS 15 requirements clarified post-go-live (FCA guidance)	Join industry working groups (UK Finance, Payments Association), participate in FCA consultations, build flexibility into systems.
PSD3 and EBA standards prove more prescriptive than expected for safeguarding	Track PSD3/PSR and EBA RTS, engage in consultations, and design safeguarding systems and governance that can absorb stricter reconciliation, diversification and reporting without major re-work.

2.6.3 Strategic Risks

RISK	MITIGATION
Member states implement PSD3 safeguarding requirements differently, fragmenting obligations for EU entities	Set a group safeguarding standard above PSD3 minimums, then layer national add-ons and centralise monitoring of local implementation.
Post-PSD3, central bank safeguarding access gives larger firms an advantage if they move balances to central banks and withdraw deposits	Define a strategy for central bank access (directly or via partners) and build value-added safeguarding services to remain competitive.

Chapter 3: PISPs & AISPs (Open Banking Providers)

This chapter consolidates regulatory obligations for Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) across UK and EU jurisdictions, which act as intermediaries between customers and banks by initiating payments or aggregating account data; pure PISPs/AISPs do not hold relevant customer funds, while EMIs/PIs with PISP permissions are in scope for safeguarding in Chapters 1-2 and are treated here only for their access and data obligations, with regulatory focus on access rights, data protection, security, and AI governance.

IN-SCOPE FIRMS	OUT OF SCOPE
• PISPs (enable third-party payment initiation via open banking) • AISPs (provide account data aggregation) • All operating in UK and/or EU	• Banks (ASPSPs, covered in Chapter 7) • Direct fintechs offering payment accounts (licensed as PIs/EMIs, safeguarding and prudential rules covered in Chapters 1-2)

3.1 Regulatory Requirements Comparison Table

PISPs/AISPs: UK vs. EU requirements (current and post-PSD3)

REQUIREMENT	UK PISPs/AISPs	EU PISPs/AISPs (PSD2 current)	EU PISPs/AISPs (PSD3 post-2027)
Access rights to bank accounts (ASPSP must provide)	✅ Required (PSD2, ongoing)	✅ Required (PSD2, ongoing)	✅ Required (PSD3/PSR, enhanced)
Bank obstacles prohibited (technical/commercial)	❌ Limited protection	❌ Limited protection	✅ Mandatory (PSD3)
API performance benchmarks (uptime, response time)	⚠️ FCA guidance only	✅ EBA technical standards	✅ EBA enhanced standards
Mobile OS access (Apple/Google NFC)	❌ No obligation	❌ No obligation	✅ Apple/Google must open (FRAND terms)
Non-discriminatory pricing (banks cannot charge PISPs more)	⚠️ FCA guidance	⚠️ EBA guidance	✅ Mandatory (PSD3)
Safeguarding obligations	❌ None for pure PISPs/AISPs (no relevant funds)	❌ None for pure PISPs/AISPs (no relevant funds)	❌ None for pure PISPs/AISPs; safeguarding sits with ASPSPs or EMIs/PIs holding balances
Liability for fraud (if PISP negligent)	✅ Own negligence only	✅ Own negligence only	✅ Own negligence only (clearer in PSD3)
Liability for account data accuracy (AISP)	✅ Protected (data from ASPSP)	✅ Protected (data from ASPSP)	✅ Protected (data from ASPSP)
Agentic AI governance	✅ Applies if deploying agentic AI	✅ Applies if deploying agentic AI	✅ Applies if deploying agentic AI
Operational Resilience (if systemically important)	✅ Yes (UK regime)	✅ Yes (EU DORA/ICT rules)	✅ Yes (EU-DORA/ICT rules)
Strategic opportunity	Constrained (bank control, uneven API quality)	Improving (regulatory pressure on access)	Favourable (stronger access, NFC opening, pricing rules)

Legend: ✅ Applies / Mandatory ⚠️ Limited / Principles-based guidance ❌ Does not apply / No obligation

Note: Where PISP permissions sit on top of an EMI/PI licence, safeguarding obligations apply to the underlying e-money/payment services, not to the PISP/AISP front-end itself.

3.2 Current Regime: UK PSRs (retained PSD2) and EU PSD2

Applies to:

- PISPs/AISPs authorised in the UK under the Payment Services Regulations 2017 (PSRs), which transpose PSD2 and now operate as retained EU law.
- PISPs/AISPs authorised in the EU under PSD2, with mandatory access to payment accounts (subject to practical obstacles that banks can still impose).

PISP/AISP obligations (current)	• Obtain and maintain technical access to ASPSP APIs • Maintain strong authentication with customers • Handle customer data securely (SCA, encryption) • UK PISPs: Manage fraud and APP reimbursement liability where they are the sending PSP for Faster Payments or CHAPS, plus liability for their own negligence and security failings • EU PISPs: Manage fraud liability for own negligence and security failings only (no APP reimbursement overlay) • AISPs (UK and EU): Manage liability for their own security failings and misuse of data • Report security incidents
ASPSP obstacles (current)	• Can rate-limit API calls ("throttling") • Can require re-authentication for each transaction (SCA friction) • Can charge discriminatory pricing (higher for PISPs than retail) • Can impose technical obstacles (API complexity, poor documentation)
PISP/AISP strategic challenges (current)	• Dependent on bank API quality and willingness • High friction for customers (repeated SCA authentication) • Profitability pressured by bank obstacles • Limited mobile wallet integration (Apple/Google control)

3.3 Post-PSD3 Regime: Enhanced Rights (EU only)

Effective Date: Estimated Q4 2027 (post-adoption and implementation)

Applies to:

- EU-operating PISPs/AISPs

Enhanced access rights, performance standards, mobile OS integration

3.3.1 Stronger Access Obligations on Banks (PSD3)

From around Q4 2027, PSD3 will put real teeth behind “access” by spelling out, in EBA standards, which technical and commercial behaviours count as forbidden “obstacles” to PISPs and AISPs. That leaves much less room for creative obstruction and turns open-banking access into regulated infrastructure rather than best-efforts plumbing.

Technical obstacles (expected to be prohibited)	**Commercial obstacles** (expected to be prohibited)
• API rate limiting ("throttling") • Requiring excessive re-authentication • Slow API response times (>1 second) • Poor API documentation • Complex authentication protocols	• Charging PISPs/AISPs more than retail customers • Exclusive partnerships restricting PISP access • Blocking PISPs from accessing certain account types • Preventing data export for customer analytics

Strategic impact for PISPs

- Reduced dependence on individual bank relationships
- Lower technical friction (better APIs, less throttling)
- Ability to build truly multi-bank experiences
- Potential disintermediation of card networks

3.3.2 Mobile Operating System Access (PSD3)

From around Q4 2027, PSD3 will require Apple and Google to open their NFC interfaces to EU-operating PISPs on Fair, Reasonable and Non-Discriminatory (FRAND) terms, turning today's tightly controlled wallets into contestable distribution. In practice, that means ending the pattern of restricted NFC on Apple, curated access on Google and piecemeal workarounds, and instead obliging both platforms to offer NFC access on commercially reasonable terms so PISPs can build their own mobile wallets and contactless journeys.

Current situation	PSD3 requirement
• Apple: Restricted NFC access (mainly Apple Pay) • Google: More permissive (Google Pay plus some competitor access) • Emerging: Some PISPs gaining limited NFC via partnerships	• Apple/Google cannot unduly restrict PISP market access • NFC must be offered on FRAND terms (not prohibitively expensive) • Enables PISPs to build mobile wallets and contactless payment journeys

Strategic impact

- PISPs can directly compete with card networks in mobile payments
- Potential disintermediation of Visa/Mastercard at point-of-sale
- Consumers choose PISP app for mobile contactless payments (not bank or card)
- Banks lose mobile wallet control (Apple/Google platform)

Implications for PISPs

- Massive opportunity (billions of consumers via Apple/Google)
- Technical complexity (NFC implementation, tokenisation)
- Regulatory compliance (PSD3 rules on liability, fraud prevention)
- Investment will vary widely depending on scope and build approach; most serious wallets require a dedicated multi-year product and engineering commitment

3.3.3 Clarified Liability Framework (PSD3)

From around Q4 2027, PSD3/PSR will clarify how fraud and data-breach liability is allocated between ASPSPs and PISPs/AISPs, while also expanding PSP fraud liability overall (for example, in impersonation scenarios). The core principle for open-banking journeys remains that PISPs are liable for losses caused by their own negligence or security failures, not for ASPSP execution failures, and that AISPs are not liable for the accuracy of account data originating from ASPSPs.

PISP liability scenarios:

✅ **PISP liable**: PISP fails to implement SCA, leading to unauthorised payment.

✅ **PISP liable**: PISP data breach exposes customer payment credentials or access tokens.

✅ **PISP liable**: PISP customer is deceived by an impersonation scam into making a payment that falls within the PSR or PSD3 reimbursement regime (for example, a qualifying employee impersonation fraud case).

❌ **PISP NOT liable**: ASPSP API is compromised where the PISP has implemented reasonable security controls.

❌ **PISP NOT liable**: Customer is deceived by a romance scam into making a payment that falls outside the PSR/PSD3 reimbursement scope.

AISP liability scenarios:

✅ **AISP liable**: AISP stores account data insecurely, leading to breach.

✅ **AISP liable**: AISP uses account data beyond the customer's authorised scope.

❌ **AISP NOT liable**: Account balance or transaction data is stale or inaccurate because of ASPSP data quality issues.

Compliance implications for PISPs/AISPs:

- Clear scope of liability (helps with insurance/indemnification)
- Emphasis on own security controls (not dependent on ASPSP security)
- Need robust incident response and audit trails

3.3.4 Agentic AI Implications (If Applicable)

An emerging question for PISPs is whether autonomous AI agents can initiate payments on behalf of customers under current or future payments rules. For example, a customer might set up an agent to "pay all my subscription bills automatically on the 1st of each month," or permit an AI to make discretionary purchases within set parameters.

Regulatory challenges:

- **Standing authority and merchant-initiated transactions**: PSD3 introduces an explicit framework for merchant-initiated transactions (MITs) following one-time SCA at mandate setup, with customers entitled to an eight-week unconditional refund right; it is unclear whether full agentic AI autonomy (for example, AI choosing amount, timing, or payee) fits within this MIT definition or requires a new legal category.
- **Consent and dynamic linking**: PSD2/PSD3 require that a payment be authorised by the payer and, for electronic payments, that SCA dynamically link the transaction to a specific amount and payee; agentic systems that select payee or amount autonomously create ambiguity around whether initial "general consent" is sufficient or whether each transaction needs fresh SCA.
- **Fraud liability allocation**: Where an AI agent makes an erroneous or fraudulent payment, it is unclear whether liability sits with the customer (as authorising party), the PISP (as executing PSP), or a new "AI operator" category; current PSD3 liability rules assume human-in-the-loop decision-making.
- **Regulatory grey area**: Neither PSD2, PSD3, nor published EBA guidance explicitly addresses fully autonomous payment agents; early guidance from the FCA AI Lab and EBA AI Act work is expected in 2026-2027, but specifics on agentic payments remain under development.

Strategic opportunity:

- Early movers that engage with regulators and pilot agentic payment use cases within well-defined guardrails (for example, capped amounts, restricted merchant categories, explicit customer opt-in) can gain competitive advantage and shape emerging standards.
- Firms that build robust audit trails, explainability, and human override mechanisms into their agentic payment architecture will find regulatory approval and customer trust easier to secure.

Premature launch of agentic AI payment features without regulatory clarity or adequate customer disclosure risks FCA or EBA enforcement action for breach of authorisation, SCA, or consumer protection rules, which is rather an expensive way to discover that regulators take a dim view of autonomous financial decision-making. The wiser path involves proactive engagement with regulators on specific use cases, participation in sandbox or AI lab programmes, and transparent communication to customers about what the AI can and cannot do on their behalf.

3.4 Priority Action Timeline

UK PISPs/AISPs (Q1-Q4 2026)

Q1-Q2 2026
(Operational Review)

ONGOING (PSD2 API Optimisation)
Review bank API performance; identify obstacles; document issues

Q1 2026
Customer Friction Assessment

- Analyse SCA re-authentication friction; plan UX improvements

Q1-Q2 2026
SCA parity & non-discrimination review

- Identify cases where ASPSPs give smoother SCA or UX to their own channels than to PISPs, document evidence, and decide which obstacles to escalate through open banking governance or to regulators.

Q1-Q2 2026
Agentic AI Assessment

- If planning autonomous payment features, engage with FCA early

Q2-Q4 2026
(Strategic Planning)

ONGOING Q2 2026 onwards (PSD3 Monitor - EU operations only)
Track EU PSD3 adoption; identify opportunities for EU PISPs

Q2-Q4 2026
Mobile Wallet Strategy

- If targeting EU market, plan for Apple/Google NFC access opportunity

Q2-Q4 2026
API outage & fallback playbook

- Define how you handle ASPSP API outages and degraded performance (customer comms, fallbacks, complaint/escalation routes) and how you evidence incidents for regulators and industry bodies.

EU PISPs/AISPs (Q2 2026-Q4 2027)

Q2 2026
(PSD3 Adoption & Opportunity Assessment)

Q2 2026 post-adoption (PSD3 gap analysis)
Assess impact of enhanced access rights, performance standards, liability clarifications

Q2-Q4 2026
Bank contract renegotiations

- Leverage PSD3 non-discrimination provisions to improve bank API terms

Q2-Q4 2026
EBA Technical Standards Monitoring

- Track ~40 expected technical standards (API performance, mobile OS, fraud prevention)

Q3-Q4 2026
(Implementation Planning)

Q3 2026 onwards (Mobile Wallet Development)
Begin mobile wallet R&D for Apple/Google NFC integration (Q4 2027 opportunity)

Q3 2026 onwards (API Infrastructure Upgrade)
Plan for enhanced ASPSP API landscape (more reliable, lower friction)

Q3 2026 onwards (Agentic AI R&D)
If planning autonomous payment agents, begin regulatory engagement with EBA and align early designs with emerging EU AI Act expectations for high-risk AI in payments (governance, oversight, explainability).

Q4 2026-Q4 2027 (Implementation & Go-Live)

Q4 2026-Q4 2027
(Implementation & Go-Live)

Q4 2026-Q4 2027
Fallback & alternative interface readiness

- Prepare to consume ASPSP fallback or alternative interfaces where required, and put processes in place to capture and evidence API downtime and obstacles under PSD3/PSR.

Q4 2027 Onwards
(Mobile wallet launch)

- Launch EU mobile wallet with NFC capability (Apple/Google FRAND access)

From Q4 2027*
PSD3 Go live benefits

- Implement leveraging enhanced access rights, performance standards, mobile OS access

2027 Onwards
Strategic Product Evolution

- Expand to account-to-account payments, bill payments, payroll integrations

** Subject to national implementation and the 18-21 month transition after 2026 adoption*

3.5 Resource Requirements

Small PISPs/AISPs (< 100k users)

UK OPERATIONS	EU OPERATIONS (current PSD2 and post-PSD3)
• Focus on a lean but capable compliance and engineering footprint to meet ongoing PSD2 obligations, maintain secure APIs, and handle incident reporting. • Day-to-day effort is concentrated on keeping connections to ASPSP APIs stable, monitoring for security incidents, and ensuring SCA and data-handling processes remain compliant.	• Expect additional one-off project work to analyse PSD3/PSR proposals, assess opportunities from enhanced access rights and mobile OS integration, and plan any mobile wallet or product enhancements. • For most smaller firms this should be managed as an incremental extension of existing teams and vendor relationships, rather than as a full-scale transformation programme.

Large PISPs/AISPs (> 1M users)

UK OPERATIONS	EU OPERATIONS (current PSD2 and post-PSD3)
• Maintain a dedicated compliance and engineering team to support high-volume API traffic, complex bank relationships, and continuous optimisation of SCA, fraud controls, and customer experience. • Larger providers will typically invest in more systematic monitoring of API performance, incident management, and AI-driven fraud detection, with formal governance over change and risk.	• Plan for a structured, multi-phase PSD3 programme covering mobile wallet development, API optimisation, and new product features that leverage enhanced access rights and Fair, Reasonable and Non-Discriminatory (FRAND)-based NFC access. • Resource needs will span regulatory analysis, product and UX design, engineering, and data teams, and should be coordinated with wider AI governance and operational resilience initiatives so PSD3 is not treated as a silo project.

3.6 Out of Scope for PISPs/AISPs

What PISPs/AISPs do NOT need to worry about:

- **Safeguarding Obligations:** Pure PISPs/AISPs do not hold customer funds, so no safeguarding requirements apply to their PISP/AISP activity. However, EMIs/PIs with PISP permissions remain in scope for safeguarding on the balances they hold (see Chapters 1-2).
- **Direct Fraud Liability (for Bank Failures):** If the bank's security is compromised, the PISP is not directly liable to the customer for execution failures. The primary liability remains with the ASPSP, with the PISP only liable where losses are caused by its own negligence or security failings.
- **App Store Obligations (Currently):** Apple/Google are not currently obligated to provide NFC access (changes post-PSD3 in EU).

What UK-only PISPs/AISPs do NOT need to worry about in 2026-2027

- PSD3 enhanced access rights, mobile OS NFC opening and related EBA technical standards will apply only in the EU; UK-only PISPs/AISPs remain under the existing PSD2-based UK open banking regime and FCA guidance.
- EU AMLR (10 July 2027) will not apply to PISPs/AISPs that have no EU customers or establishments; UK AML obligations continue instead.
- EU-specific consumer protection changes under PSD3 (for example spending limits and new liability nuances) will affect EU PISPs/AISPs, not firms operating solely under the UK regime.

3.7 Risk Factors & Mitigation

This is not a full enterprise risk register. It is a focused list of ways PISPs and AISPs can still be caught out even if they follow the rest of this roadmap. The scope is narrow on purpose: regulatory curve-balls, operational snags, and a few strategic headwinds that are specific to open-banking providers in a PSD3 world, not every generic "fintech risk" your board already worries about.

Regulatory Risks

RISK	MITIGATION
PSD3 requirements differ from current market expectations	Monitor EBA technical standards closely, participate in consultations, engage with regulators early.
Agentic AI creates regulatory pushback if launched prematurely	Early regulatory engagement (pre-launch), clear customer consent frameworks, liability insurance.

Operational Risks

RISK	MITIGATION
Bank API throttling or deliberate obstacles limit PISP growth (pre-PSD3)	Document obstacles, report to FCA/EBA, negotiate contracts with performance SLAs. Prepare to use the strengthened anti-obstacle toolkit under PSD3/PSR once live.
Apple/Google fail to open NFC on reasonable terms post-PSD3	Regulatory coordination with the European Commission and relevant NCAs if FRAND or DMA-style requirements are breached.

Strategic Risks

RISK	MITIGATION
Incumbent banks and card networks lobby against PSD3 enforcement	Participate in industry working groups (fintech associations), engage with regulators
PSD3 benefits are captured by "super-aggregators", leaving smaller PISPs as commodity API clients.	Differentiate beyond raw API connectivity (for example through vertical specialisation, analytics, UX, or niche segments), and use industry alliances/standards to avoid being locked into unfavourable aggregator or platform dependencies.

3.8 Key Takeaways

If you only remember four things from this chapter as a PISP or AISP, make them these:

- **For UK-only PISPs/AISPs**, the next two years are about squeezing more out of the existing PSD2-based UK open banking regime: reduce SCA friction, push back on unjustified API obstacles, and treat outage and incident handling as a core product feature, not a back-office chore.

- **For EU PISPs/AISPs**, PSD3 is an opportunity play as much as a compliance one: stronger access rights, FRAND-based NFC access, and clearer liability rules reward firms that are ready with mobile wallet strategies, better SLAs and differentiated services when the regime starts to bite from late 2027 onwards.

- **Pure PISPs/AISPs** stay out of safeguarding and direct bank-failure liability, but they face rising expectations on security, incident reporting, AI governance and customer consent, especially if they move into agentic or semi-autonomous payment journeys.

- **The biggest strategic risk** is not that PSD3 arrives, but that its benefits accrue to a handful of super-aggregators; PISPs and AISPs that win will specialise, build superior UX or analytics, and avoid being just another commodity API client.



Chapter 4: Cryptoasset Firms

This chapter consolidates regulatory obligations for cryptoasset service providers and stablecoin issuers across UK and EU jurisdictions. Cryptoasset firms face a dual-regime challenge: UK FSMA 2023 regime, now implemented through the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (go-live 25 October 2027, with a 30 September 2026 to 28 February 2027 authorisation gateway) and EU MiCAR (phased implementation 2024–2026), plus interaction with PSD3 (EU, post-2027) if issuing stablecoins qualifying as e-money.

IN-SCOPE FIRMS	OUT OF SCOPE
• **Cryptoasset Service Providers (CASPs)**: centralised exchange, custody, brokerage and portfolio-management providers acting as identifiable intermediaries (for example CEXs, custodial wallets, brokerages) • **Stablecoin issuers** (asset-referenced tokens, e-money tokens) • All serving UK and/or EU customers	• Traditional payment institutions offering ancillary crypto services (covered in Chapters 1-2) • Purely decentralised finance (DeFi) protocols with no identifiable CASP or issuer acting as an intermediary. • Non-custodial / self-custodial wallet providers that do not control client private keys and do not otherwise perform MiCAR-listed cryptoasset services. • Blockchain infrastructure providers (for example miners, node operators, validators) that • are not providing regulated cryptoasset services to customers.

What UK-only crypto firms do NOT need to worry about in 2026-2027:

- **MiCAR and PSD3 interaction apply only where you have EU customers or entities**; a crypto firm serving only UK customers from the UK is outside the scope of MiCAR and PSD3, and should focus on FSMA 2023 authorisation and UK AML rules.
- **EU AMLR (10 July 2027) will not apply to UK-only cryptoasset firms with no EU operations**; UK Money Laundering Regulations (MLRs) remain the primary AML/CFT framework.
- **EU PSD3-based e-money treatment for stablecoins matters only if you issue euro- or EU-facing e-money tokens**; a UK-only stablecoin issuer is concerned instead with the UK Qualifying Stablecoins regime under FSMA 2023.
- **This comfort does not extend to overseas firms that directly target UK retail clients from abroad**; it mainly applies where you are genuinely UK-only or where any UK business is routed entirely through a UK-authorised intermediary.



4.1 Regulatory Requirements Comparison Table

Cryptoasset Firms: UK FSMA vs. EU MiCAR vs. PSD3 Interaction

REQUIREMENT	UK FSMA 2023	EU MiCAR	EU PSD3 (if stablecoin = e-money)	Post-2027 UK/EU divergence / strategic notes
Authorisation required	✅ Yes (CASP or Qualifying Stablecoin Issuer)	✅ Yes (CASP or Crypto Asset Issuer)	✅ Potentially (if e-money token)	Both regimes are mandatory but structurally different; UK is a standalone regime, EU firms may face dual MiCAR+PSD3 licensing if issuing e-money-like stablecoins.
Go-live / application timing	25 October 2027 regime go-live; priority gateway 30 Sep 2026-28 Feb 2027 for existing firms	Phased go-live 2024-2026 (already in force for many services)	Q4 2027 onwards, after 2026 adoption and an 18-21 month transition	UK firms can use a defined gateway window to secure transitional protections; EU firms are already largely in-regime and now preparing for PSD3 overlay.
Application gateway	✅ Priority gateway 30 Sep 2026-28 Feb 2027 (transitional protections if inside window)	❌ N/A (MiCAR already live; no equivalent gateway)	❌ N/A	UK has an "early preparation" advantage for currently active firms; EU firms instead faced earlier MiCAR transition.
Stablecoin classification	Qualifying Stablecoins under FSMA 2023 (separate UK regime)	EMTs (e-money tokens) and ARTs (asset-referenced tokens)	EMTs may also qualify as e-money under PSD3, triggering dual MiCAR+PSD3 treatment	Frameworks diverge: UK keeps a separate qualifying-stablecoin regime; the EU splits EMT/ART in MiCAR and layers PSD3 on e-money-like tokens.
Custody / safeguarding requirements	UK-specific crypto custody and safeguarding rules for CASPs and qualifying stablecoins	MiCAR-specific custody and wallet standards for cryptoassets	PSD3 safeguarding obligations if the token meets the e-money definition	Safeguarding approaches differ, and larger EU issuers may shift part of their safeguarding model to PSD3 (including potential central bank options) while UK issuers stay in the FSMA track.
PSD3 interaction	❌ None (UK is separate; no PSD3)	⚠️ Indirect: MiCAR is primary, but PSD3 matters if issuing EMTs that are also e-money	✅ Direct where stablecoin qualifies as e-money (PSD3 e-money framework applies on top of MiCAR)	UK remains isolated from PSD3; EU stablecoin issuers face more complex dual-compliance (MiCAR + PSD3), especially for EMTs.
AML supervision	FCA under UK MLRs	National AML supervisors today; EU AMLA will directly supervise systemically important firms from 10 July 2027	EU AMLR and AMLA overlay AML expectations for MiCAR/PSD3 entities	UK firms focus on UK MLRs and FCA expectations; EU firms must plan for direct EU-level AML supervision and harmonised AMLR rules on top of national regimes.
Cross-border operations	Separate authorisations needed for EU; no passport into EU markets	MiCAR passport: one EU authorisation covers all member states	PSD3 passport for e-money/payment services, if applicable	EU firms gain single-market reach under MiCAR/PSD3 passports; UK-only firms must choose between staying domestic or layering EU authorisations.
Transitional provisions	✅ Transitional protections available for firms applying via the UK gateway window	⚠️ Transitional MiCAR provisions largely phased out during 2024-2026	❓ TBD (dependent on final PSD3/PSR text)	Both regimes require sustained investment; UK firms can plan against a clear pre-2027 gateway, while EU firms focus on embedding MiCAR and preparing for AMLR/PSD3 overlaps.

Legend: ✅ Applies / Mandatory ⚠️ Conditional / Interaction depends on activity ❌ Does not apply / No obligation

4.2 UK Crypto Regime (FSMA 2023)

Effective Date: 25 October 2027 (go-live)

Applies to:

- Firms conducting in-scope cryptoasset activities from a place of business in the UK
- Most international firms serving UK retail clients (with the FCA generally expecting a UK-incorporated entity for retail-facing business, although branch models may be considered case-by-case)
- Cryptoasset Service Providers (CASPs)
- Qualifying Cryptoasset Issuers (stablecoin issuers meeting UK criteria)

Note: International firms that serve only UK professional clients, or route their UK business entirely through a UK-authorised intermediary, should not normally be required to obtain separate authorisation under the new cryptoassets regime, but will need to monitor how the FCA interprets "professional client" in practice.

4.2.1 Authorisation Categories

CASP vs Cryptoasset Issuers

In practice, UK crypto regulation treats trading venues and custodians very differently from the firms that actually issue "money-like" tokens. The two categories below show which side of that line you sit on, and what that means for your licence.

Dimension	Cryptoasset Service Provider (CASP)	Qualifying Cryptoasset Issuer
Scope	Exchange, custody, brokerage, portfolio management.	Stablecoin issuers meeting UK-specific qualifying-stablecoin criteria.
Definition	Firm providing regulated cryptoasset services (for example operating a trading venue, brokerage, or custodial service) to UK customers.	Digital asset designed to maintain stable value, typically via fully backed collateral reserves that meet FSMA 2023 requirements.
Authorisation	FCA authorisation required (CASP permissions under FSMA 2023).	Separate regime and permissions from CASPs (issuer authorisation as a Qualifying Cryptoasset Issuer).
Prudential / reserve requirement	Capital requirement proportionate to assets under custody/management (no specific "100% reserve" obligation on customer assets beyond custody rules).	100% reserve in specified assets (for example fiat currency and other eligible liquid assets) held in line with rules for qualifying stablecoins.
Safeguarding/ Custody	Client cryptoassets must be segregated from firm assets, with robust key-management, record-keeping, and wind-down planning, under the FCA's cryptoasset custody regime.	Backing assets for qualifying stablecoins must be held with appropriate custodians, segregated and ring-fenced from the issuer's own assets, with clear legal rights for token holders over the reserve pool.
Redemption rights	Not applicable (no obligation to redeem tokens at par; obligations centre on safe custody and conduct of business).	Holders have the right to redeem qualifying stablecoins for fiat at par value, subject to the conditions set out in FSMA 2023 and FCA rules.
Insurance	Professional indemnity insurance required, in line with FCA expectations for CASPs.	May be required or expected depending on business model (for example to cover operational and conduct risks), but the primary protection is the reserve and redemption framework.
Examples	Centralised exchange, custodial wallet provider, automated trading platform.	Fiat-backed stablecoins (for example 1:1 GBP or other fiat backing) that meet the qualifying-stablecoin test; algorithmic designs are explicitly out of scope for this regime.

While FSMA 2023 defines its own "qualifying stablecoin" category, many UK firms will also have EU-facing tokens. The table below is a quick cross-reference, showing how typical stablecoin types line up under the UK regime, under MiCAR (EMT/ART), and under PSD3's e-money test.

UK vs. EU stablecoin definitions:

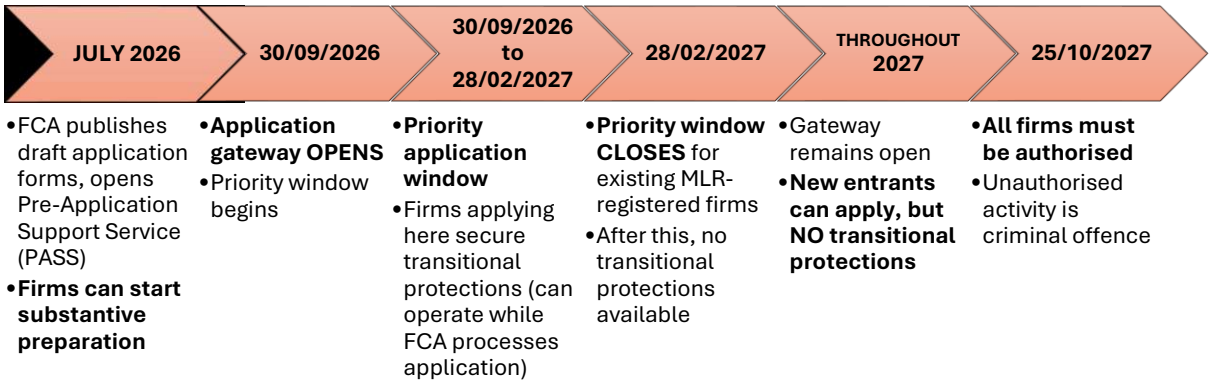
Aspect	UK (Qualifying Stablecoins)	EU (EMT/ART)	Interaction with PSD3
Fiat-backed	✅ Covered	✅ E-money token (EMT)	✅ Qualifies as e-money (PSD3) if meets definition
Asset-backed (non-fiat)	⚠️ Possible (TBD)	✅ Asset-ref. token (ART)	❌ Does NOT qualify as e-money
Algorithmic	❌ Explicitly excluded (UK policy)	❌ Not treated as EMT/ART under MiCAR	N/A

4.2.2 UK Gateway Process (CRITICAL)

Think of the gateway as the one-time fast lane into the new UK crypto regime. If you are already serving UK customers, this is your chance to lock in continuity and avoid discovering on 25 October 2027 that you are suddenly on the wrong side of the perimeter.

Timeline

The dates below are not just milestones in an FCA project plan. They are the difference between a managed transition into the FSMA regime and a last-minute scramble to keep your UK business open.



Why the gateway matters:

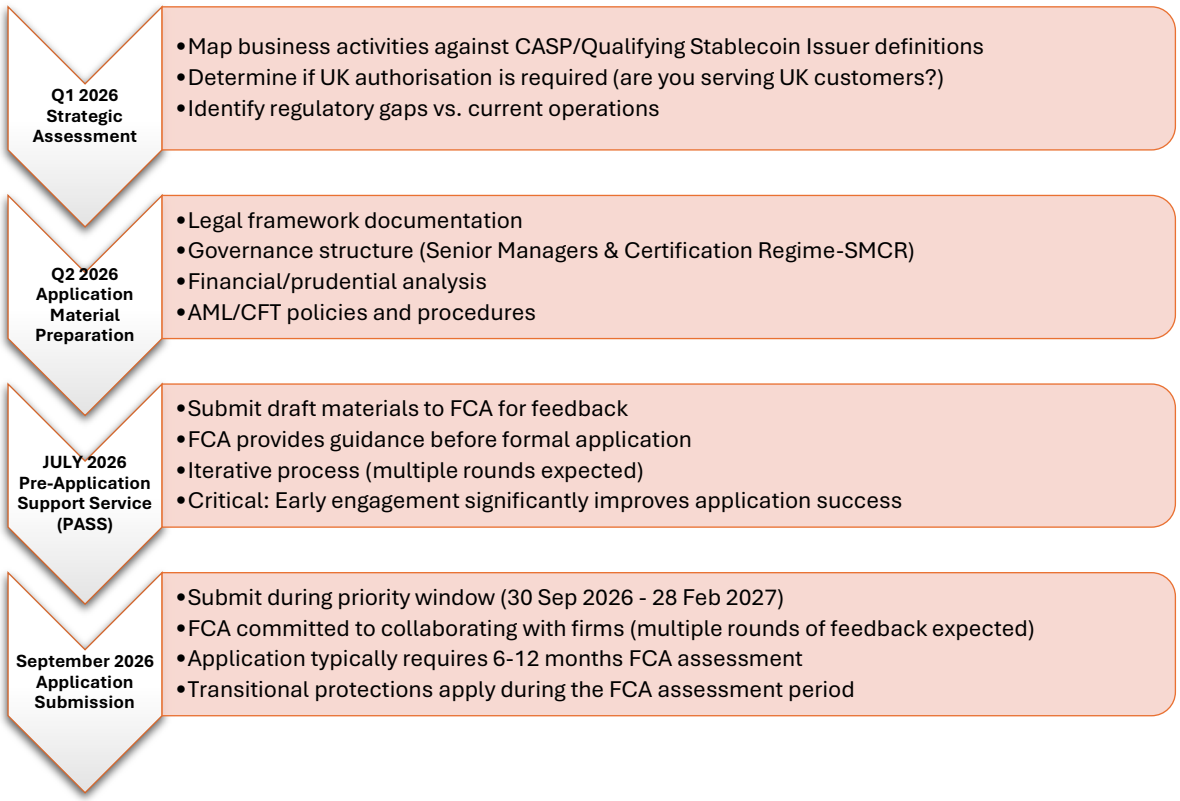
1. **Pre-commencement authorisation**: FCA aims to determine priority applications BEFORE 25 October 2027 go-live

2. **Business continuity**: Firms applying during window can continue operating through authorisation process

3. **25 October 2027 is a hard stop**: firms that have not applied via the gateway must cease UK crypto activities and can no longer rely on an FCA-authorised s.21 approver route for cryptoasset promotions.

4.2.3 Application Preparation (Critical Path)

Getting through the gateway is less about heroics in September 2026 and more about boring, disciplined prep in the months before. The steps below show what you need to have done, and by when, if you want your application to glide rather than crash-land.



4.2.4 Life After Authorisation: Ongoing Obligations

Getting through the gateway is not the finish line; it is the point at which the hard, unglamorous work becomes day-to-day. Once authorised, crypto firms are expected to behave like any other regulated financial institution, with clear accountability, resilient operations, and no corners cut on AML or customer protection. Once authorised, your firm must be able to demonstrate:

- **SMCR Senior Manager accountability** (a named senior manager responsible for crypto activities, with clear documentation of their role and oversight).
- **AML/CFT reporting** (robust customer due diligence, suspicious activity reporting, and accurate beneficial-ownership verification).
- **Custody and safeguarding of client crypto** (assets held securely, segregated from the firm's own balance sheet, with clear entitlement records). The FCA is also working on bringing crypto custody into a CASS-style client-asset framework, so firms should expect their arrangements to be tested against CASS-type standards rather than informal practice.
- **Consumer protection** (fair and clear disclosures, compliant financial promotions, effective complaint handling, and FOS jurisdiction where applicable).
- **Operational resilience** (incident reporting, tested business-continuity arrangements, and cyber/ICT resilience that meets regulatory expectations).
- **Ongoing FCA supervision readiness** (timely regulatory reporting, openness to audits and thematic reviews, and evidence that supervisory findings are acted on).
- **Market abuse and disclosure**: For firms operating trading venues or arranging trading in qualifying cryptoassets, this includes surveillance for insider dealing and manipulation, detailed audit trails and escalation procedures, and admission-to-trading and disclosure standards aligned with traditional securities markets.

4.3 EU MiCAR Regime

Phased Implementation: 2024-2026 (already underway)

Applies to:

- All firms providing cryptoasset services in EU member states
- Cryptoasset Service Providers
- Crypto Asset Issuers (EMT and ART issuers)

Most MiCAR requirements are now live and in force, and national transitional periods end by 1 July 2026 at the latest, after which CASPs without MiCAR authorisation must stop in-scope services in the EU.

4.3.1 UK vs. EU Detailed Comparison

For firms active on both sides of the Channel, MiCAR and the UK FSMA regime are two separate, overlapping worlds. The table below is a quick sense-check of where they align, where they diverge, and where they make your life more complicated.

ASPECT	UK FSMA REGIME	EU MICAR	IMPLICATION
Geography	UK customers only	EU member states	Separate applications required
Go-live date	25 October 2027	Phased (2024-2026, mostly live)	EU-authorised firms should already be compliant; UK-authorised firms have more runway before FSMA go-live
Gateway process	Yes (Sep 2026 - Feb 2027)	No (already live)	UK advantage: Preparation time
Stablecoin regime	Qualifying Stablecoins (separate)	EMT/ART (separate)	Divergent frameworks
e-money interaction	None (UK separate)	YES (PSD3 overlap for EMTs)	EU more complex
Safeguarding	UK-specific custody rules	MiCAR custody rules	Different operational requirements
AML supervision	FCA	AMLA + National (dual for systemically important)	EU dual supervision adds burden
Application process	Iterative (FCA works with firms through gateway and assessment)	Single authorisation process with national regulator (passport once approved)	UK process is more iterative; EU process is more formalised once authorised
Transitional protections	Yes (gateway window)	Phased out (ongoing)	UK new entrants have time; EU changing

4.3.2 MiCAR Categories

MiCAR draws a sharp line between service providers and token issuers, and then splits issuers into EMT and ART regimes with very different obligations. The table below summarises how those three categories work in practice so firms can map their current and planned activities onto the right authorisation and control set.

Dimension	Cryptoasset Service Provider (CASP)	E-Money Token (EMT) Issuer	Asset-Referenced Token (ART) Issuer
Scope/ Definition	Exchange, custody, brokerage, execution and portfolio management services for clients in EU member states, authorised to provide one or more MiCAR "crypto-asset services" (for example trading platform, custody, execution, advice).	Issues tokens referencing a single official currency, intended as a means of exchange and meeting MiCAR EMT tests (for example a fiat-backed euro or dollar stablecoin issued by an EU e-money/payment institution or bank).	Issues tokens referencing a basket of non-fiat or mixed assets (for example commodities or indices) and meeting MiCAR ART tests (for example a multi-asset stablecoin backed by a basket of commodities or indices).
Authorisation	Authorised as a CASP by the national competent authority of an EU member state.	Authorised either as a credit institution or as an e-money institution/payment institution authorised to issue EMTs under MiCAR and related sectoral rules.	Authorised as an ART issuer under MiCAR (separate issuer authorisation), in addition to any CASP authorisations if services are also provided.
Passporting	Once authorised as a CASP in one member state, can passport services across the EU (subject to notification).	EMTs issued by an authorised entity can be offered across the EU, subject to MiCAR passport/notification requirements and any local add-ons.	ARTs issued by an authorised issuer can be offered across the EU, subject to MiCAR passport/notification requirements and any local add-ons.
Prudential / reserve requirement	Capital and organisational requirements set at CASP level (no dedicated "100% reserve" requirement, but custody and client-asset rules apply where relevant).	100% backing of outstanding EMTs with eligible reserve assets, plus prudential and governance requirements drawn from e-money/payment-services and MiCAR frameworks.	Specific reserve, governance and risk-management requirements tailored to the reference asset basket, with more focus on market and liquidity risk than pure fiat-backing.
Safeguarding/ Custody	If providing custody/administration, must meet MiCAR custody standards (segregation, safekeeping, record-keeping, and recovery/wind-down planning).	Reserve assets and customer entitlements must be safeguarded under EMT rules, often via credit institutions or other permitted custodians.	Reserve assets and customer entitlements must be safeguarded under ART rules, including custody of underlying reference assets and redemption mechanisms.
PSD3 Interaction	Indirect only: CASPs are primarily MiCAR firms; PSD3 matters if they also hold a PSD3 licence (for example as a payment institution) alongside MiCAR permissions.	EMTs may also qualify as e-money under PSD3, creating dual MiCAR+PSD3 compliance (for example PSD3 e-money safeguarding and passporting on top of MiCAR).	ARTs do not qualify as e-money under PSD3 (only EMTs do), so PSD3 does not apply to the token itself, though it may apply to other services the issuer provides.
Redemption rights	No MiCAR-mandated redemption right at par; CASPs act on client instructions for trades, deposits and withdrawals.	Statutory right to redeem at par in the reference currency, backed by detailed redemption-plan and crisis-management requirements.	Right to redeem in funds or, where allowed, in underlying/referenced assets, with MiCAR/EBA rules on redemption plans and stress events.
Insurance	No single MiCAR insurance rule; firms are expected to use insurance or equivalent risk-transfer (for example PI, cyber, crime) for operational and liability risks.	Insurance cannot replace full reserves, but PI, D&O, cyber or crime cover may form part of the operational-risk framework, scaled to issuance size.	Given higher prudential and governance expectations, insurance or similar tools are used to mitigate operational and liability risks around complex reference-asset baskets and redemptions.

4.3.3 Key Compliance Obligations (EU)

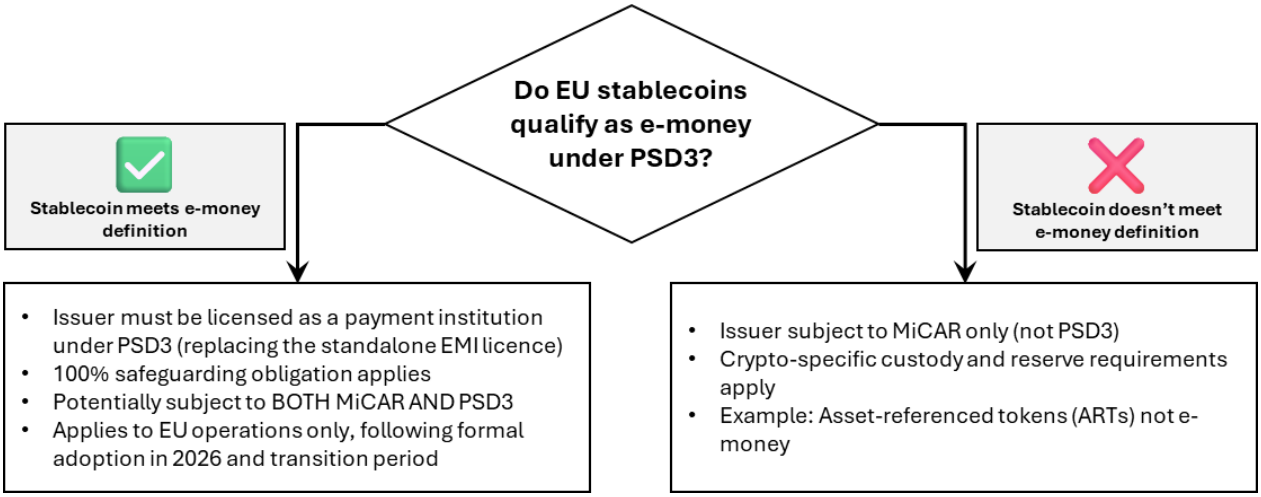
MiCAR is not a one-off licence event. It is an ongoing set of behaviours regulators expect to see baked into your day-to-day operations. Think of the bullets below as the minimum “always-on” settings you cannot switch off once you are in the MiCAR club.

- Authorisation from national regulator
- Custody/safeguarding of customer cryptoassets
- AML/CFT reporting (under existing national AML rules, with EU AMLR and AMLA adding an EU-level layer from 10 July 2027)
- Consumer protection and disclosures
- Operational resilience and incident reporting
- Ongoing supervision (can include direct AMLA supervision for systemically important firms from 10 July 2027)



4.3.4 PSD3 Interaction (EU Stablecoin Issuers Only)

PSD3 is where MiCAR's stablecoins meet the traditional payments rulebook. Before you choose a licence, you need to decide whether your token really walks and talks like e-money. The diagram below shows what to look out for:

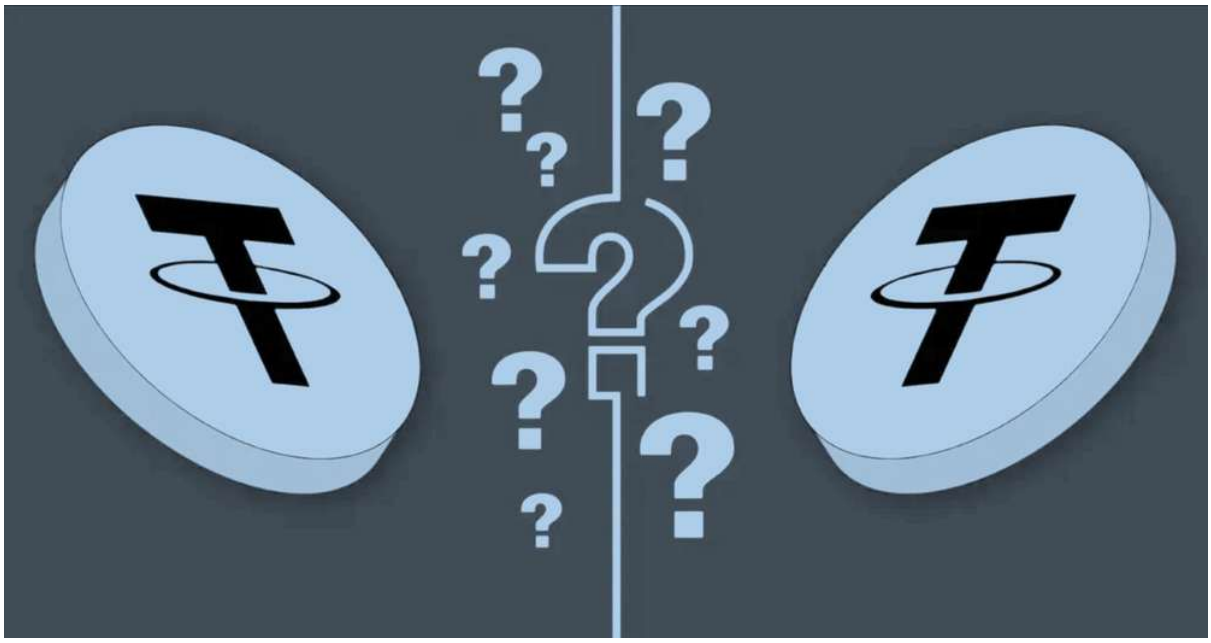


PSD3/ EMD2 merger impact:

- EMD2 being repealed and integrated into PSD3
- e-money issuance will be integrated into PSD3/PSR framework
- Payment Institutions will be able to issue e-money without separate EMI license
- Simplifies licensing for firms issuing both fiat e-money and stablecoins
- Does not affect UK (UK EMIs remain under EMRs 2011)

Strategic implication for EU stablecoin issuers:

- Major licensing uncertainty until PSD3 final text published (Q2 2026 expected)
- Once adopted, EU stablecoin issuers may need to transition from EMI + MiCAR to PI + PSD3
- Or, if ART (asset-referenced token), remain MiCAR-only
- Either way, significant compliance work required in 2026-2027



4.4 Priority Action Timeline

Regulators have set the clocks. 4.4 is your playbook for using the time left in 2026 and 2027 wisely, rather than discovering the deadlines when the door is already closing.

4.4.1 All Crypto Firms (Q1-Q3 2026 - UK and EU)

IMMEDIATE Q1-Q2 2026
UK Authorisation Preparation

- Scoping analysis: Map business activities against CASP / Qualifying Stablecoin Issuer definitions.
- Gateway readiness: Prepare for 30 September 2026 opening.
- Application window critical: Plan to submit between 30 Sep 2026 and 28 Feb 2027.
- Pre-Application Support Service (PASS): Engage with FCA starting July 2026.
- Draft application forms: Review when published (July 2026) and begin substantive preparation.
- Early engagement with FCA (July-September 2026) significantly improves success rate.
- Engage external legal counsel for a joined-up UK-EU crypto compliance and licensing strategy if also operating in the EU.

Q2-Q3 2026
Strategic Assessment (EU operations)

- PSD3/MiCAR interaction: Assess if stablecoins qualify as e-money under PSD3 (EU operations only).
- Monitor stablecoin classification: Track how each token is treated across MiCAR EMT, PSD3 e-money and UK qualifying stablecoin regimes.
- Section 21 reliance ending: Prepare for loss of third-party s.21 approver route to UK market (ends 25 October 2027).
- EU MiCAR compliance: Ensure ongoing compliance with phased MiCAR implementation.

4.4.2 UK Crypto Firms (Q3-Q4 2026)

The detailed UK gateway dates and application steps are set out in sections 4.2.2 (Gateway process) and 4.2.3 (Application preparation); firms should treat those as the primary playbook for Q3-Q4 2026.

4.4.3 EU Crypto Firms (Q2 2026-Q4 2027)

Q2 2026
PSD3 Adoption

- **PSD3 final text**: Published (estimated Q2 2026)
- **Gap analysis**: Assess impact of e-money token = e-money classification (if applicable to your stablecoins)
- **Licensing strategy**: Determine if MiCAR-only, PSD3-only, or dual compliance required

Q4 2026-Q2 2027
Transition Planning

- **PSD3 technical standards**: Track EBA development of technical standards for safeguarding, fraud prevention
- **Licensing plan**: Develop transition roadmap if dual compliance required (MiCAR + PSD3)

Q3-Q4 2027
Implementation

- **PSD3 go-live**: Full implementation (expected Q4 2027, 21-month transition period post-adoption)
- **EU AMLR effective**: 10 July 2027 (direct EBA supervision for systemically important firms)

4.4.4 All Crypto Firms (2027 Ongoing)

MID-2027 ONWARDS

- **25 October 2027 (UK)**: UK FSMA crypto regime fully live - any firm serving UK customers must be authorised from this date.
- **From 25 October 2027 (UK)**: Carrying on in-scope UK cryptoasset activities without authorisation becomes a criminal offence.
- **10 July 2027 (EU)**: 10 July 2027 (EU): EU AMLR applies - crypto firms with EU operations must comply with the new EU-level AML framework and, where designated, prepare for direct supervision by the EU AMLA.
- **Late 2027 into 2028 (EU)**: For EU stablecoin issuers and CASPs, MiCAR obligations should be fully embedded and PSD3 obligations implemented where tokens qualify as e-money or where payment-service activities are in scope.

4.5 Resource Requirements

4.5.1 Small Crypto Firms (< £10M annual volume)

UK AUTHORISATION PROGRAMME	EU MiCAR COMPLIANCE (If applicable)
• Smaller firms will typically treat UK FSMA authorisation as a substantial but focused change initiative, centred on scoping, documentation, governance design, and control build-out ahead of the gateway window. • Most of the work will sit with founders/senior management, a compliance lead, and external legal or regulatory advisers, with targeted input from technology and operations to evidence custody and resilience arrangements. • In practice, this usually means a small, part-time UK change team rather than a standalone programme office, with budgets focused on advisory time and control uplift rather than major platform rebuilds.	• For firms already operating in the EU, MiCAR should now be embedded into day-to-day operations; the main resourcing need is ongoing monitoring of developments and periodic enhancements to disclosures, custody, and reporting. • Small firms should aim to converge their UK and EU governance and control frameworks over time, rather than running completely separate compliance approaches.

4.5.2 Large Crypto Firms (> £500M annual volume)

UK AUTHORISATION PROGRAMME	EU MiCAR COMPLIANCE (If applicable)
• Larger firms will generally run UK FSMA authorisation as a full regulatory change programme, with dedicated workstreams for governance/SMCR, prudential analysis, custody/safeguarding, AML/CFT, and operational resilience. • This typically requires sustained involvement from senior executives, central programme teams, risk and compliance functions, specialist legal counsel, and product/technology leaders.	• For EU operations, MiCAR obligations should already be in force; the forward focus is on ensuring consistent application across entities and preparing for direct AMLR supervision where relevant. • Large firms may also need to evaluate PSD3 implications for any e-money-like stablecoin activity, and plan licensing and restructuring work accordingly.

4.5.3 Dual UK/EU firms

- Firms active in both UK and EU markets should treat UK FSMA authorisation, MiCAR, PSD3 (where applicable), and AMLR as a single regulatory portfolio, with a coherent target operating model rather than separate regional solutions.
- The main resourcing challenge is coordination: aligning governance, risk, and control frameworks so that policy, monitoring, and reporting can operate on a "build once, apply many times" basis across jurisdictions.

4.6 Critical Success Factors

Spreadsheets won't get you authorised. This section pulls out the few levers that actually change your odds of getting through FSMA and MiCAR/PSD3 in one piece.

RISK	MITIGATION
Early Engagement (Q1-Q2 2026)	The FCA emphasised firms must be "substantively prepared" at point of submission. Waiting until September 2026 gateway opening is too late. Early preparation and PASS engagement significantly improves authorisation outcomes.
Regulatory Intelligence	Monitor: • FCA PASS feedback (July 2026 onwards) • EBA technical standards development (EU) • PSD3 final text (EU, Q2 2026 expected)
Dual-Jurisdiction Strategy	For firms operating UK + EU: • Parallel application streams (UK + EU) • Harmonised governance/compliance frameworks • Centralised regulatory monitoring
Internal ownership and accountability	Clear internal ownership: Assign a named senior manager for the UK FSMA authorisation workstream and, where relevant, a counterpart for EU MiCAR/PSD3 so responsibility is not diffused across product, legal and ops.
Banking and safeguarding relationships (for custodial models)	Safeguarding and banking partners: Lock in relationships with UK safeguarding banks/custodians and, for EU operations, any key MiCAR/EMT reserve custodians early, as limited market capacity can become a bottleneck close to go-live.

4.7 Risk Factors & Mitigation

Regulatory Risks

RISK	MITIGATION
Missing the UK gateway window and ending up unauthorised for UK crypto business in late 2027	Treat gateway preparation as a 2026 change programme, with scope agreed early, real PASS engagement, and a latest safe submission date inside the priority window.
Underestimating PSD3/AMLR impacts on EU stablecoins and CASPs after MiCAR	Run a second-wave impact review once texts are final to identify e-money-like tokens, extra PSD3 licences and new AMLR supervision implications.
Running separate UK and EU control stacks with inconsistent policies and reporting	Design one core governance and control framework that satisfies FSMA, MiCAR and (where relevant) PSD3/AMLR, then add thin local variations only where needed.
Mis-scoping which entities need which licences in which jurisdictions	Map activities, entities and customer locations explicitly, then align licences and control ownership to that map rather than to legacy structures.

Operational Risks

RISK	MITIGATION
Authorisation pack and governance not "supervisor-ready" at submission	Dry-run the file internally or with advisers so board materials, policies, prudential analysis, custody and AML can withstand detailed challenge.
Custody and key-management controls below MiCAR/FSMA expectations	Harden segregation, reconciliations and key-management, and get an independent review; treat custody as a client-assets function, not just tech.
AML systems not scaled for higher-risk crypto and potential EU-level AMLR oversight	Tune KYC, EDD and monitoring for crypto typologies, and make sure file-level decisions are well-evidenced and reproducible.

Reputational Risks

RISK	MITIGATION
Being seen as a "reluctant complier" by FCA or EU supervisors	Engage early, meet milestones, and use pre-application channels constructively rather than pushing everything to the deadline.
Confusing customer communications about authorisation status and regime changes	Prepare a clear, consistent story for UK and EU customers on what is changing and when, and align it with your actual licences and prudential position.

4.8 Key Takeaways

In practice, this chapter leaves leadership with four hard asks for 2026-2027.

- UK-only crypto firms have one non-negotiable job in 2026: arrive at the **gateway** "substantively prepared", submit between 30 September 2026 and 28 February 2027, and be fully authorised by 25 October 2027 or exit the UK market.
- EU-facing firms must treat **MiCAR as BAU** from now on and use 2026-2027 to work out whether any of their tokens "walk and talk" like e-money, because that determines whether PSD3 turns into a second, overlapping licence.
- Dual-jurisdiction firms cannot afford two separate crypto control stacks; the winning move is a **single governance and control framework** that satisfies FSMA, MiCAR and (where relevant) PSD3/AMLR, with only thin local tailoring.
- For smaller players, success is about **focus**, not armies: a tight core of founders/senior management, one strong compliance lead and the right external counsel will get you much further than a sprawling, under-directed project team.



Chapter 5: BNPL Providers

Scope Statement

This chapter consolidates regulatory obligations for Buy Now Pay Later (BNPL) providers across UK and EU jurisdictions. BNPL is classified as consumer credit (not payment services), creating a separate regulatory framework from PSD2/PSD3. UK and EU implementations differ materially, notably, the UK has a merchant financing exemption not present in the EU.

Stakeholders covered:

- Third-party BNPL lenders (Klarna, Clearpay, PayPal BNPL, etc.)
- Banks offering BNPL products
- Fintechs offering BNPL as primary business
- All serving UK and/or EU customers

Out of scope:

- Merchants offering BNPL directly (UK exemption only, not regulated as finance providers)
- Credit cards and traditional credit products (separate consumer credit framework)
- Point-of-sale lending (separate regulatory scope)

5.1 Regulatory Requirements Comparison Table

BNPL Providers: UK vs. EU requirements.

Legend: ✅ Applies / mandatory ⚠️ Conditional / model dependent ❌ Does not apply / exempt.

Dimension	UK BNPL Regulation (FCA)	EU BNPL Regulation (Consumer Credit Directive - national implementation)	Post-2026 divergence
Effective date	✅ 15 July 2026	✅ 20 November 2026	⚠️ Different timelines and slightly different scope
Regulatory authority	✅ FCA (consumer credit)	✅ National regulators in each member state (directive implemented locally)	⚠️ Each member state implements separately; supervision and enforcement more fragmented than in the UK
Authorisation required	✅ FCA authorisation or variation of permission for consumer credit/BNPL	✅ Lender must be authorised by the relevant national authority	✅ Both regimes require authorisation in principle, but firms face one UK process vs multiple EU processes
Merchant exemption	✅ YES - merchants financing their own sales exempt from BNPL authorisation (UK policy choice)	❌ NO - no general merchant exemption; merchants offering BNPL typically in scope	⚠️ UK is materially more lenient for merchant-offered BNPL; EU merchants face higher regulatory cost
Loan type covered	✅ Interest-free short-term BNPL credit	✅ Interest-free OR low-interest short-term BNPL credit	⚠️ EU may capture a broader set of instalment products depending on national implementation
Typical term limit	✅ Typically < 12 months (short-term instalments)	✅ Typically < 12 months (short-term instalments), set in national rules	⚠️ Similar overall, but member-state choices can tighten or relax limits at the margin

Dimension	UK BNPL Regulation (FCA)	EU BNPL Regulation (Consumer Credit Directive - national implementation)	Post-2026 divergence
Creditworthiness assessment	✅ CONC 5.2A affordability-based assessment, proportionate to ticket size	✅ Affordability/ creditworthiness assessment under national rules implementing the directive	⚠️ Intent is aligned (affordability), but methodologies, proportionality thresholds and documentation expectations differ by jurisdiction
Pre-contract information (SECCI)	✅ SECCI form must be provided before the contract is agreed	✅ SECCI form mandatory, harmonised across the EU and localised into national languages	⚠️ Form is harmonised, but language and delivery expectations are more fragmented across EU markets
Unfair contract terms	✅ UK unfair contract terms regime applies to BNPL agreements	✅ EU Unfair Contract Terms Directive applies via national law	⚠️ Principles are similar, but enforcement practice and case law differ between the UK and individual EU states
Complaint handling / redress	✅ FCA complaint-handling rules + FOS jurisdiction	✅ National complaint-handling rules and ombudsman/ arbitration schemes; ❌ no single EU-wide FOS equivalent	⚠️ UK offers a single Ombudsman route; EU redress landscape is more fragmented and varies by market
Adequate explanations (adverse decisions)	✅ Meaningful explanations required where credit is refused or terms changed on an automated basis, plus reconsideration routes	✅ Equivalent requirement in national law for explanations when credit is refused or altered	⚠️ Both regimes are converging on meaningful, non-boilerplate explanations, but practical expectations differ by supervisor
AI governance (credit decisioning)	✅ AI governance and explainability expectations being built out around BNPL underwriting, layered on top of Consumer Duty	✅ AI governance for BNPL decisioning will sit under the EU AI Act's "high-risk AI" framework from 2027 onwards	⚠️ Both push towards stricter governance and explainability, but via different legal instruments and timelines
Data protection	✅ GDPR plus UK expectations on data use, transparency and Consumer Duty	✅ GDPR EU-wide, with additional national guidance in some markets	⚠️ GDPR baseline is common, but the UK overlays Consumer Duty and the EU overlays the AI Act; cross-border firms must track both layers
Cost to comply	⚠️ Material but highly variable; driven by portfolio size, technology maturity and reuse of existing credit processes	⚠️ Material but highly variable; depends on number of EU markets, local divergence and reuse of existing frameworks	⚠️ In both cases BNPL regulation is a significant change programme, not a minor policy tweak; there is no single benchmark cost

5.2 UK BNPL Regulation (FCA)

Effective Date: 15 July 2026

APPLIES TO	DOESN'T APPLY TO
• Third-party BNPL lenders serving UK customers • Banks offering BNPL products • Fintechs offering BNPL	• Merchants offering BNPL directly (UK exemption - merchants financing own sales) • Credit cards, overdrafts, other consumer credit products (separate framework)

FCA Policy Statement (Q1 2026)

A final FCA Policy Statement is expected in Q1 2026 and will confirm the detailed perimeter, permission categories and transitional arrangements for BNPL lenders. Firms should treat that Statement as the definitive source on which permissions they need, whether a transitional route is available to them, and any additional conditions attached to BNPL authorisation.

5.2.1 Authorisation Requirement

UK BNPL rules treat third-party BNPL as regulated consumer credit, not as a payment service, and bring these lenders fully into the FCA's authorisation and conduct regime from 15 July 2026.

DIMENSION	FCA AUTHORISATION	VARIATION OF PERMISSION	TRANSITIONAL PERMISSION / TPR FOR BNPL
Scope	Unauthorised firms that want to start offering BNPL to UK customers.	Existing consumer-credit firms adding BNPL or bringing BNPL clearly into scope.	Existing BNPL/ deferred-payment providers that qualify for a time-limited regime while moving onto full permissions.
Definition	Full FCA authorisation for consumer-credit lending, including BNPL.	Change to an existing permission so BNPL is explicitly covered.	Temporary permission that lets in-scope firms keep trading while their full authorisation/variation is assessed.
Core authorisation requirement	Obtain new permissions covering "consumer credit lending" and the relevant BNPL/deferred-payment activities.	Secure a variation of permission so BNPL products and journeys sit within the current credit licence.	Submit a compliant application, meet entry criteria and complete authorisation/variation before the regime ends.
When used	No current FCA consumer-credit permission.	Consumer-credit permission already held, but BNPL is new or materially different.	Already operating BNPL and brought into scope of the new regime with an FCA transitional route.
Typical timeline	~3-6 months for assessment of a substantively complete pack.	Often shorter than a new authorisation, but still plan for several months.	Limited by the regime's end-date/application window; underlying full/variation application still typically ~3-6 months.
Examples	Fintech with only payments/e-money permissions launching BNPL; retailer creating a standalone BNPL lender.	Bank authorised for cards/loans adding BNPL; lender rebadging instalment products as BNPL.	Existing BNPL provider allowed to rely on temporary permission while its full or variation application is processed.

Requirement (Mandatory by 15 July 2026):

- All third-party BNPL lenders must either obtain full FCA authorisation for consumer-credit lending or secure a variation of permission that clearly covers BNPL.
- Carrying on in-scope BNPL lending after 15 July 2026 without the relevant FCA permission will be a criminal offence.

5.2.2 Creditworthiness Assessments (CONC 5.2A)

The FCA's Consumer Credit sourcebook (CONC) sets the rules for UK lending. CONC 5.2A is the section that requires firms to assess a customer's creditworthiness - including both affordability and credit risk - before they enter into, or significantly vary, a regulated credit agreement. From 15 July 2026, BNPL lenders are fully in scope: they must apply the same proportionate creditworthiness standards to BNPL as to any other consumer-credit product, not just run a quick score check.

The table below summarises what this means in practice for BNPL providers.

Dimension	Requirement for BNPL lenders
Effective date	Mandatory from 15 July 2026.
Timing	Affordability must be assessed **before** granting BNPL credit or increasing a BNPL limit.
Data you cannot rely on alone	Credit reference data on its own is not sufficient - it must be part of a broader assessment.
Factors that must be considered	Income and regular expenditure; other debts and financial commitments; family status and dependants; employment status; and any foreseeable changes that could affect affordability.
Standard: proportionality	Assessment must be proportionate to the size, cost and risk of the BNPL agreement - small tickets (e.g. £100) can use simplified checks, but they still need to be real affordability assessments, not superficial "computer says yes" approvals.
Practical data sources	Credit reference agencies; open banking data for income and outgoings; internal behavioural data; and customer-provided information.
Operational capabilities	Systems to perform and record affordability checks; manual override capability for edge cases; clear decision rules that can be explained and defended.
Documentation & audit trail	For each decision, firms should be able to show what information was used, how it was weighed, and why the outcome (approve/decline/limit) was reasonable.
Compliance & resourcing	Implement or upgrade affordability assessment systems; train staff on CONC 5.2A; review and, where needed, redesign existing BNPL decisioning logic; expect a meaningful one-off uplift in spend on systems, training and model validation.

In practice, this means building affordability checks into BNPL journeys as a hard control rather than an add-on, with systems, data sources and staff training all aligned so that firms can evidence fair, proportionate decisions if the FCA asks.

5.2.3 Pre-Contract Information (SECCI Form)

From 15 July 2026, BNPL agreements are subject to the same pre-contract information rules as other regulated credit: firms must give customers a Standard European Consumer Credit Information (SECCI) form before they commit.

SECCI requirements for BNPL providers

DIMENSION	REQUIREMENT FOR BNPL LENDER
Effective date	Mandatory from 15 July 2026.
When SECCI must be provided	Before the customer commits to a BNPL contract (i.e. pre-contract, not after confirmation).
Nature of the form	Standard European Consumer Credit Information (SECCI) template; harmonised across UK/EU, with prescribed headings and ordering.
Key information SECCI must include	Creditor name and contact details; total amount of credit; duration of the agreement; repayment schedule (dates and amounts); total amount payable (for interest-free BNPL this equals the credit amount); APR (0% for interest-free BNPL but still disclosed); consequences of non-payment; customer's right to withdraw.
Product and journey design implications	Product marketing and checkout flows must surface SECCI clearly before commitment, not bury it in small print or post-contract emails.
Accuracy and readability	SECCI content must be accurate, complete and in plain English; firms should test whether typical customers actually understand it.
Language requirements	Where selling to non-English speakers, SECCI should be provided in appropriate languages, consistent with how the product is marketed.
Systems and documentation	Systems must generate the correct SECCI for each product, capture delivery/acceptance in the audit trail, and keep versions aligned with product changes.
Compliance and cost implications	Expect one-off spend to update systems, templates and customer journeys, plus ongoing effort to maintain SECCI accuracy and periodically test customer understanding.

In practice, that means treating SECCI as part of the BNPL product experience, not just a legal attachment: it has to appear at the right moment, in language customers can understand, and in a form your systems can evidence if challenged.

5.2.4 Adequate Explanations

Requirement (Mandatory from 15 July 2026):

- If credit refused or terms amended based on automated decision (AI credit scoring), must provide explanation
- Explanation must be meaningful and not just "computer says no"
- Consumer has right to request reconsideration

Compliance implications:

- Review AI credit decisioning logic (ensure explainability)
- Design customer-facing explanations (clear, non-technical)
- Establish reconsideration process (human review of appeals)
- Expect focused investment in adapting credit decisioning systems, building explainability capabilities, and establishing a workable appeals process for customers impacted by automated decisions.

5.2.5 Merchant Exemption (UK-specific)

In the UK, the law cuts merchants some slack: if you're simply spreading the cost of your own goods, you're treated very differently from a specialist BNPL lender.

Policy Decision: Merchants offering BNPL directly are EXEMPT

Rationale:

- Avoid burdening small retailers with FCA authorisation costs
- Distinguish between specialist credit providers and merchants offering payment flexibility

Definition of exempt merchant:

- Merchant financing own sales (customer buys from merchant, merchant offers payment plan)
- NOT: Merchant partnering with third-party BNPL provider (then third-party is regulated)

Examples:

✅ **EXEMPT**: High-street clothing retailer offering own customers 3-month payment plan on £200 purchase

❌ **REGULATED**: Klarna, Clearpay (third-party BNPL providers)

⚠️ **GRAY AREA**: Large e-commerce platform offering own-label BNPL to customers (may be treated as BNPL provider if platform also finances purchases of other merchants)

Unlike the EU, which generally pulls merchants offering BNPL into its consumer-credit regime, the UK carves them out, leaving third-party lenders in the regulatory spotlight and giving UK merchants a modest cost advantage over their EU peers.

5.2.6 Financial Ombudsman Service (FOS) Jurisdiction

Requirement (Effective 15 July 2026)

From 15 July 2026, BNPL customers will be able to escalate eligible complaints to the Financial Ombudsman Service if they are unhappy with a firm's final response or if the firm fails to respond within the required timeframe. FOS decisions are binding on BNPL firms up to the applicable compensation limits in force at the time of the award. Under the FCA Handbook, the Dispute Resolution: Complaints sourcebook (DISP) sets out how firms must handle complaints and interact with FOS.

In practice, this means BNPL providers must operate a DISP-compliant internal complaints process, participate in FOS (including paying case fees and any relevant levies), and ensure staff understand FOS processes and expectations. Firms should also plan for a non-trivial ongoing cost of handling ombudsman cases and implementing any awards or systemic recommendations that follow from them.

5.3 EU BNPL Regulation (Consumer Credit Directive)

Effective Date: 20 November 2026

Scope:

- BNPL providers operating in EU member states
- EU-incorporated lenders and non-EU lenders serving EU customers
- Implementation and supervision handled by national regulators in each member state

How the EU approach differs from the UK:

- No general merchant exemption: merchants offering BNPL are typically brought into the consumer-credit regime.
- Supervision is national, not via a single EU conduct authority.
- Dispute resolution is member-state specific; there is no EU-wide equivalent of the UK Financial Ombudsman Service.
- Detailed rules and expectations (affordability thresholds, term limits, disclosure norms) vary by country.

ASPECT	LIKELY VARIATION BY MEMBER STATE
Affordability assessment standard	Differences in how strictly proportionality is applied, and what evidence is expected for small-ticket BNPL.
Merchant exemption	Some states may consider limited carve-outs; others may bring most merchant-offered BNPL fully into scope.
Maximum term	Certain markets may cap interest-free or low-interest BNPL at shorter terms (for example, under 12 months).
Dispute resolution	Different ombudsman or arbitration schemes, with varying powers and procedures.
Language requirements	SECCI and other disclosures must appear in the national language(s); expectations on readability and prominence may differ.

For cross-border BNPL providers, this means one core compliance framework will need local add-ons for affordability, term limits, language and complaints handling in each target market.

5.4 Priority Action Timeline

UK BNPL Providers (Q1-Q3 2026)



- **FCA Policy Statement**: Expected early Q1 2026 with final rules, to be treated as the definitive playbook for permissions, any transitional routes, and detailed conduct requirements
- **Authorisation assessment**: Determine if existing FCA authorisation covers BNPL or variation required
- **Application preparation**: If not currently authorised, begin FCA application process
- **CONC 5.2A readiness**: Review creditworthiness assessment requirements
- **Creditworthiness frameworks**: Implement affordability assessments (CONC 5.2A standards)
- **Pre-contract disclosures**: Update product documentation with SECCI forms
- **Adequate explanations**: Prepare systems for providing explanations of credit decisions
- **FOS preparation**: Ensure complaint handling readiness for FOS jurisdiction
- **Regulatory compliance:** All systems, processes, disclosures operational
- **Staff training:** Ensure frontline and operations teams trained on CONC obligations
- **Monitoring and reporting:** Establish ongoing compliance monitoring
- **Fraud monitoring**: Monitor fraud trends, adjust controls as needed
- 2**Fair lending review**: Audit credit decisioning for bias and fairness (prepare for Consumer Duty / AI governance scrutiny)
- **FOS preparedness**: Monitor emerging FOS decisions on BNPL and be ready to adjust policies and processes as early case law develops

EU BNPL Providers (Q2-Q4 2026)



- **National regulator engagement:** Identify how each EU member state implementing BNPL rules
- **Member state variations:** Assess which markets BNPL provider operating in, map local requirements
- **Affordability framework localisation:** Design proportionate assessment for each member state
- **SECCI translation:** Prepare multilingual SECCI forms
- **20 November 2026:** EU BNPL rules effective across member states
- **Phased rollout:** Implement market-by-market (if operating across multiple member states)
- **Dispute resolution setup:** Establish national dispute resolution engagement for each market

All BNPL Providers (Q4 2026-2027)



- **FCA AI guidance:** Prepare for AI governance expectations expected to crystallise by around December 2026 (UK)
- **Credit decisioning explainability:** Review Consumer Duty obligations for algorithmic underwriting
- **Fraud detection bias:** Assess fairness and de-banking risk in fraud AI models
- **EU AI Act (EU providers):** Prepare for December 2027 effective date
- **FCA Consumer Duty embedding:** Ongoing compliance (UK providers)
- **Post-quantum cryptography:** Monitor emerging standards for payment data encryption

For most BNPL providers, the pattern is one intense 2026 build-out (permissions, CONC, SECCI, FOS), followed by a 2027 horizon where AI governance and cross-border EU Consumer Credit Directive implementation become the main moving parts.

5.5 Resource Requirements

Small BNPL Providers (< £50M credit outstanding)

UK REGULATION (BY 15 JULY 2026)	EU REGULATION (BY 20 NOVEMBER 2026)
• Smaller providers will typically treat BNPL regulation as a focused change programme, centred on FCA authorisation (or variation of permission), basic creditworthiness systems, and alignment with CONC. • Most of the work will sit with compliance, underwriting, and operations teams, supported by technology changes to capture SECCI disclosures and adequate explanations within customer journeys.	• Single-market providers can usually adapt existing consumer credit processes to meet BNPL rules, with targeted updates for affordability, disclosures, and complaint handling in the relevant member state. • Governance effort is largely about understanding national implementation detail and making sure frameworks are localised appropriately, rather than building new infrastructure from scratch.

Large BNPL Providers (> £500M credit outstanding)

UK REGULATION (BY 15 JULY 2026)	EU REGULATION (BY 20 NOVEMBER 2026)
• Larger providers will tend to run BNPL as a full regulatory change programme, integrating authorisation, CONC 5.2A affordability, Consumer Duty, AI governance, and FOS readiness into a single workstream. • Expect dedicated resource from compliance, risk, product, data science, and technology, with more formal programme management and board-level oversight.	• Multi-market providers need to plan for country-by-country implementation, with central standards and local variations for affordability, disclosures, and dispute resolution. • Coordination between central policy teams and in-country operations will be critical to avoid divergent implementations and duplicated effort.

Dual UK/EU Providers:

- Firms active in both the UK and EU should approach BNPL regulation as a single portfolio, mapping common elements (creditworthiness, disclosures, AI governance) and then layering the UK-specific merchant exemption and EU member-state nuances on top.
- The main resourcing challenge is less the absolute volume of work and more sequencing and coherence: avoiding building two parallel compliance stacks when one well-designed framework can be adapted across markets.

5.6 Out of Scope for BNPL Providers

BNPL providers live in the credit universe, not the plumbing cupboard: CASS 15, PSD2/PSD3 and card-scheme rulebooks only bite where a group entity also acts as a payment institution, e-money institution, bank, card issuer or acquirer. Pure BNPL lending itself sits under the consumer-credit stack (CONC, SECCI and, in the EU, CCD II[15]), not under the payment-services and safeguarding frameworks that keep everyone else awake at night.

5.7 Risk Factors & Mitigation

Regulatory Risks

RISK	MITIGATION
FCA enforcement on affordability assessments (inadequate testing)	Robust affordability testing (pre-go-live), documentation of testing results, ongoing monitoring of arrears/forbearance outcomes, and senior manager oversight.
FCA Consumer Duty enforcement (credit decisioning bias)	Regular bias testing, diverse testing panels, audit AI-driven decisioning, and maintain a documented fair-lending and Consumer Duty governance framework.
EU member state implementations diverge significantly	Early engagement with national regulators in each member state, and CCD II-aware system design that allows for localised affordability, APR and disclosure rules.
Product design causes harm (repeat use, fee-heavy variants, or misleading "0%" messaging)	Formal product-governance process (including vulnerable-customer lens), testing of marketing and UX for clarity, and periodic outcome reviews (repeat-use patterns, arrears, complaints).
Misinterpreting UK or EU CCD II perimeter and licensing requirements	Early, jurisdiction-by-jurisdiction legal scoping of BNPL models; clear mapping of which entity is creditor in each market; periodic perimeter reviews as FCA rules and CCD II transposition evolve.

Operational Risks

RISK	MITIGATION
Affordability assessment system fails pre-go-live	Extensive UAT (user acceptance testing), parallel manual processes during transition.
SECCI forms non-compliant with consumer expectations (low readability)	Consumer testing of SECCI forms (regulators expect plain language), ongoing monitoring of complaints and drop-off rates, and iterative design.

Reputational Risks

RISK	MITIGATION
High-profile FOS case against BNPL provider (affordability/credit decisioning)	Strong internal controls, well-documented decision-making that can be evidenced to FOS, and a robust fair-lending programme.

5.8 Key Takeaways

If you only remember four things from this chapter as a BNPL provider, make them these:

- **For UK lenders, 2026 is authorisation plus affordability**, not just a bit of paperwork. You either have the right consumer-credit permission (or variation) in place by 15 July 2026 or you stop lending, and from that date every BNPL journey needs a real CONC-standard affordability check, a SECCI form and a complaints process that can withstand FOS scrutiny.
- **For EU BNPL players, CCD II is less a single rulebook than a family of dialects**. You get one core set of rights and obligations but different affordability thresholds, term caps, disclosure nuances and redress routes in each member state, so any serious cross-border model needs "local plug-ins", not a one-size-fits-all template.
- **Across both markets, the real regulatory heat will be on product design and outcome**s, not just legal drafting. Repeat-use patterns, fee-heavy variants and misleading "0%" messaging will draw Consumer Duty and CCD II attention just as quickly as bad documentation, especially where vulnerable customers are involved.
- And underneath it all, **your reputation will be built or broken in the data trail**: robust, explainable credit decisions, well-run complaints and FOS cases, and a clear story on fairness and bias are what will separate the BNPL providers regulators can live with from the ones they quietly decide to make an example of.



Chapter 6: Acquirers

Scope Statement

This chapter consolidates regulatory obligations for merchant acquirers across the UK and EU jurisdictions. Acquirer obligations depend entirely on business model, and specifically how funds are held and settled. Four distinct models create fundamentally different regulatory obligations. This chapter focuses on statutory and regulatory obligations (for example CASS 15, PSD3/PSR, operational resilience, AML and fraud/APP liability where relevant). Card scheme rules (such as Visa and Mastercard rulebooks) apply separately and continue to bind scheme-member acquirers, but they are not analysed in detail here.

Stakeholders covered:

- **Bank-licensed acquirer**: Merchant settlement directly to merchant bank accounts; no acquirer-held payment accounts.
- **PI-licensed acquirer (no fund holding)**: Payment Institution; funds immediately settled (T+0/T+1); no suspense/float.
- **PI-licensed acquirer (with fund holding)**: Payment Institution; holds merchant funds (suspense accounts, rolling reserves, split payments).
- **EMI-licensed acquirer**: E-Money Institution; merchants hold e-money balances; 100% of merchant e-money is safeguarded where the EMI, not a partner bank, is the issuer.
- All operating in UK and/or EU

Out of scope:

- Card scheme settlement flows (inter-bank, not customer funds)

In a nutshell:

Safeguarding Obligation	Model A (Bank-Licensed)	Model B (PI, no fund holding)	Model B (PI, with fund holding)	Model C (EMI)
UK Safeguarding	Bank regime (no CASS 15 as PI/EMI).	Out of scope for CASS 15 if no relevant funds held at end of business day.	CASS 15 applies to relevant merchant funds from 7 May 2026.	CASS 15 applies to 100% of safeguarded e-money balances from 7 May 2026.
EU Safeguarding	Covered by bank prudential rules, not EMD2/PSD2/PSD3 safeguarding.	Out of scope if no relevant funds held; still need to confirm flows do not create end-of-day balances.	PSD2 safeguarding of relevant funds today; moves into harmonised PSD3 safeguarding from ~2027 onwards.	EMD2 safeguarding of 100% of issued e-money today; moves into merged PI/EMI PSD3 safeguarding from ~2027 onwards.
In Practice	Merchant card proceeds settle bank-to-bank; acquirer does not maintain merchant payment accounts.	Acquirer never holds relevant funds at end of business day (same-day pass-through, no suspense/float).	Acquirer holds merchant funds in own-name accounts (suspense, rolling reserves, split pay, multi-day settlement).	Acquirer issues e-money to merchants; merchant balances are e-money, not pure settlement funds.

The next sections will explain this in more detail.

6.1 Regulatory Requirements Comparison Table

Acquirers: Business Model Determines Obligations

Legend: ✅ Applies / Mandatory ⚠️ Conditional/ Model dependent ❌ Does not apply/ exempt

DIMENSION	BANK-LICENSED	PI - NO FUND HOLDING	PI - WITH FUND HOLDING	EMI-LICENSED
UK Safeguarding (CASS 15)	❌ Bank prudential/client money rules instead.	❌ Out of scope if no relevant funds are held at end of business day.	✅ Safeguard merchant funds held in PI accounts.	✅ Safeguard 100% of merchant e-money balances held by the EMI.
EU Safeguarding (EMD2 / PSD2 / PSD3)	❌ Covered by CRD/CRR style bank rules, not EMD2/PSD2/PSD3 safeguarding.	❌ Out of scope if no relevant funds are held at end of business day.	✅ PSD2: safeguard 100% of relevant funds; PSD3: moves into harmonised PI safeguarding.	✅ EMD2: safeguard 100% of e money; PSD3: merged PI/EMI safeguarding after transition.
UK CoP (Confirmation of Payee)	⚠️ If FPS/CHAPS participant and offers merchant sending accounts.	⚠️ If PI is FPS/CHAPS participant and offers merchant sending accounts.	⚠️ If PI is FPS/CHAPS participant and offers merchant sending accounts, regardless of fund holding.	⚠️ If EMI is FPS/CHAPS participant and offers merchant sending accounts.
EU VoP (Verification of Payee)	⚠️ If executing credit transfers for merchant settlement.	⚠️ If executing credit transfers for merchant settlement.	⚠️ If executing credit transfers for merchant settlement, even where funds are held.	⚠️ If executing credit transfers for merchant settlement.
PSD3 Fraud Prevention (EU)	⚠️ If providing PSD3-in-scope merchant payment accounts (beyond pure card acquiring).	✅ For EU acquiring/payment services in PSD3 scope.	✅ For EU acquiring/payment services in PSD3 scope, alongside safeguarding duties.	✅ For EU acquiring/payment services in PSD3 scope, plus e money safeguarding.
Operational Resilience (UK & EU)	⚠️ Where the bank is in scope of UK/EU operational resilience or ICT/DORA regimes.	⚠️ Where the PI meets size/importance thresholds for those regimes.	⚠️ Where the PI meets thresholds; fund holding typically increases supervisory focus.	⚠️ Where the EMI meets thresholds; safeguarded balances often increase scrutiny.
AI Governance (underwriting, fraud)	✅ AI for merchant onboarding and fraud must meet explainability/ fairness/ oversight expectations.	✅ AI for merchant onboarding and fraud must meet explainability/ fairness/ oversight expectations.	✅ AI for merchant onboarding and fraud must meet explainability/ fairness/ oversight expectations, with attention to fund holding risk drivers.	✅ AI for merchant onboarding and fraud must meet explainability/ fairness/ oversight expectations across acquiring and e-money activity.
AML / Merchant risk controls	✅ Bank AML regime applies; acquirer underwriting and monitoring in scope.	✅ PI AML obligations apply to acquiring activity.	✅ Fund holding increases focus on merchant due diligence.	✅ EMI AML obligations across acquiring and e-money, including merchants.
PSD3 Open Banking (EU)**	⚠️ Only if acting as ASPSP for merchant payment accounts in PSD3 scope.	⚠️ Only if providing merchant payment accounts that fall under PSD3 and must be exposed via APIs.	⚠️ Only if providing merchant payment accounts that fall under PSD3 and must be exposed via APIs, whether or not funds are held.	⚠️ Only if providing merchant payment accounts that fall under PSD3 and must be exposed via APIs.
Strategic position	Lightest specific safeguarding burden if you stay out of PSD3 acquiring.	Lean model if you keep true T+0/T+1 settlement.	Extra features (reserves, split payments) without full EMI weight.	"Gold standard" trust/safety proposition, especially post PSD3.

** For acquirers, UK CoP only bites where the acquiring entity also operates FPS/CHAPS-enabled sending accounts for merchants; many acquirers will be out of scope in practice, but that comes from their rails and account set-up, not from being a bank vs PI vs EMI.*

*** "Merchant payment accounts" means payment accounts as defined in PSD2/PSD3 (for example current-account-like products), not bare card-settlement flows without an ongoing account relationship.*

Key observations:

1. Business model is determinative: Fund holding classification drives safeguarding obligations
2. Immediate end-of-day pass-through = no safeguarding: If relevant funds do not remain with the acquirer at the end of the business day, CASS 15 safeguarding does not apply.
3. Suspense/float accounts = safeguarding obligation: triggers CASS 15 in the UK and PSD2/EMD2 today (moving into PSD3) in the EU
4. E-Money model = highest compliance burden: 100% safeguarding of merchant e-money required
5. Geographic split: UK CASS 15 only applies to UK operations; EMD2 (and then PSD3/PSR) applies to EU operations

In other words, acquirers don't all live under the same storm cloud: if you're a bank acquirer you mostly live with APP fraud and resilience; if you're a PI you only really suffer once you start holding merchant money; and if you're an EMI you've volunteered for the full safeguarding workout, with all the scrutiny (and trust) that comes with it. If you want to see how that plays out in real life, the next section walks through each model in turn.

6.2 Three Acquirer Business Models Detailed

Before diving into the detail, start by identifying which of the three models you actually run in practice: a bank-licensed acquirer with pure pass-through settlement, a PI acquirer that may or may not hold merchant funds, or an EMI acquirer running full e-money balances. The following sections walk through each model in turn so you can map your current flows, licences and safeguarding duties without needing a separate legal memo.

6.2.1 Model A: Bank-Licensed Acquirers

Typical structure:

- Bank-licensed entity or subsidiary of bank (e.g. Barclaycard Merchant Services)
- Merchant settlements flow directly to merchant bank accounts
- No holding of merchant funds in proprietary payment accounts
- Card scheme settlements via inter-bank mechanisms (not customer funds)

Regulatory scope

✅ IN SCOPE FOR	❌ OUT OF SCOPE FOR
• Operational resilience (if systemically important) • AI governance (merchant underwriting, fraud detection) • UK CoP (if CHAPS/Faster Payments participant for settlement) • EU VoP (if executing credit transfers for merchant settlement)	• UK Safeguarding CASS 15 (bank prudential regime applies) • EU Safeguarding (EMD2/PSD2/PSD3) (bank prudential regime applies)

Compliance implications:

- Minimal incremental compliance cost, as the core bank prudential and conduct regimes already apply.
- Legal scoping is still required to confirm that settlement flows do not create safeguarding obligations and to validate operational resilience expectations.
- Expect a focused but contained spend on external legal input and any operational resilience reviews needed to document the position, rather than a full-scale change programme.

Strategic advantage:

- The acquiring business avoids the additional PI/EMI safeguarding stack for acquiring, because they're already inside the bank's prudential regime.

6.2.2 Model B: PI-Licensed Acquirers (Payment Institution)

Typical structure:

- Licensed as Payment Institution (PSRs 2017 UK / PSD2-PSD3 EU) (e.g. acquired.com)
- May or may not hold merchant funds (business model variant)
- If no fund holding: funds settled to merchant bank accounts on the same business day (no balances held overnight).
- If fund holding: funds held beyond the day of receipt (for example suspense accounts, rolling reserves, split payment accounts).

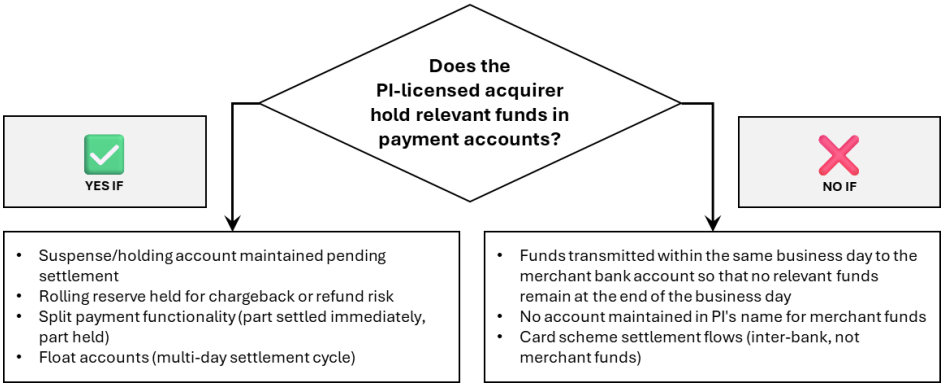
Regulatory scope (NO fund holding)

✅ IN SCOPE FOR	❌ OUT OF SCOPE FOR
• PSD3 fraud prevention and transparency (if EU operations) • Operational resilience (if systemically important) • AI governance (merchant underwriting, fraud detection)	• Safeguarding of end-of-day merchant balances (model is designed so that no relevant funds remain at the end of the business day).

Regulatory scope (WITH fund holding)

✅ IN SCOPE FOR	❌ OUT OF SCOPE FOR
• CASS 15 safeguarding (UK operations, if holding relevant merchant funds) • PSD3 safeguarding (EU operations, from 2027 onwards), building on existing PSD2/EMD2 safeguarding obligations • PSD3 fraud prevention and transparency (if EU operations) • Operational resilience (if systemically important) • AI governance	

The diagram below shows you what to look out for:



Compliance implications (with fund holding)

- Follow Payment Institution guidance (Chapter 1)
- CASS 15 implementation required (May 2026 deadline for UK)
- PSD3 preparation (Q2 2026 onwards for EU building on existing PSD2 safeguarding obligations)
- firms should plan for a more structured safeguarding workstream CASS 15 in the UK and PSD3 safeguarding in the EU, including reconciliation, governance, and audit changes rather than treating this as a light-touch policy update. Expect a meaningful but still bounded spend on external legal advice, safeguarding design, and limited systems change, rather than a wholesale rebuild of the acquiring platform.

Compliance implications (no fund holding)

- Minimal ongoing safeguarding operations, but firms must still document how settlement flows avoid end-of-day client balances and comply with any intra-day safeguarding expectations.
- PSD3 fraud prevention compliance (EU only)
- incremental compliance cost is limited to legal scoping of settlement flows and confirming that safeguarding is not triggered because no balances are held overnight, plus any PSD3 fraud-prevention obligations for EU operations.

Strategic advantage (with fund holding)

- Ability to **support higher-risk and more complex merchants** through rolling reserves, split-pay, and structured settlement models.
- Scope to build richer value-add products (e.g. reserves-backed risk terms, marketplace and platform payouts) that can justify higher pricing.
- Stronger protection against chargebacks and refunds, enabling more confident growth in higher-risk segments.

Strategic advantage (no fund holding)

- **Lean acquiring model** with lower safeguarding overhead, because no merchant balances are held beyond the business day of receipt.
- Attractive to merchants needing faster cash-flow, as same-day settlement improves working capital.
- Simpler wind-down and failure scenarios, which is easier to explain to boards, investors, and regulators.

6.2.3 Model C: EMI-Licensed Acquirers (E-Money Institution)

Typical structure:

- Licensed as E-Money Institution (EMRs 2011 UK / EMD2-PSD3 EU) (e.g. checkout.com)
- Merchants hold e-money balances in accounts
- Provides both card acceptance AND stored value services
- 100% of merchant e-money issued must be safeguarded

Regulatory scope:

✅ **IN SCOPE FOR** (Full obligations)	❌ **OUT OF SCOPE FOR**
• CASS 15 safeguarding (UK operations, for safeguarded merchant e-money balances) • PSD3/PSR safeguarding (EU operations, when implemented) • PSD3 fraud prevention and transparency (if EU operations) • Operational resilience (if systemically important) • AI governance (merchant underwriting, fraud detection)	

Compliance implications

- Follow E-Money Institution guidance (Chapters 1-2)
- Highest compliance burden of three models
- CASS 15 implementation required (May 2026 for UK)
- PSD3 transition planning (during 2026 and 2027 for EU)
- Expect a substantial, multi-workstream investment across safeguarding design, systems change, audit readiness, and PSD3 transition work, closer to a full regulatory change programme than a light-touch policy refresh.

Strategic advantage

- Higher customer trust (100% safeguarding)
- Potential differentiation in merchant base
- Post-PSD3: central bank safeguarding option (deposit risk eliminated)

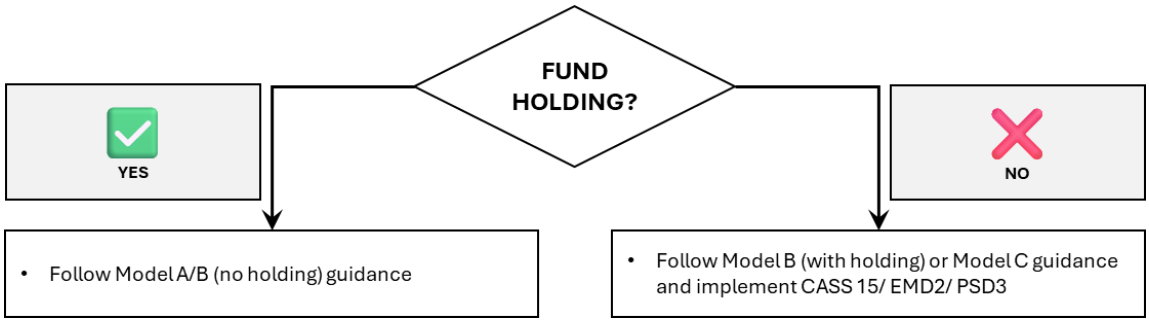
6.3 Priority Action Timeline

All Acquirers (Q1 2026 - Immediate)

CRITICAL (Q1 2026): Legal Scoping

- **Conduct legal analysis:** "Does our business model hold relevant funds subject to safeguarding?"
- **Document business model:** Map funds flows, settlement cycles, account types
- **Engage legal counsel:** Confirm CASS 15 applicability (UK) and EMD2/PSD3 implications (EU)
- If in scope, **confirm UK operational resilience and AI governance expectations for acquiring** (important business services, incident reporting, and AI use in merchant underwriting and fraud).

The following decision tree shows you which model to follow:



Model B (with fund holding) / Model C Acquirers (Q1-Q2 2026)

CRITICAL (by 7 May 2026): CASS 15 Implementation (UK)

- Follow Payment Institution / E-Money Institution action plan (Chapters 1-2).
- Focus on: daily reconciliation systems, audit engagement, resolution pack, SMCR designation.

Note: design, banking arrangements and policy work must be underway well before 7 May 2026 to meet the live date.

Q1-Q2 2026 (EU operations): Early PSD3/VoP/AMLR scoping

- Confirm whether you provide EU-facing payment accounts or execute credit transfers for merchant settlement (drives PSD3 fraud/VoP scope).
- Start PSD3 gap analysis for safeguarding and fraud obligations alongside core PI/EMI work in Chapters 1-2.
- For EU entities, assess high-level AMLR impacts on existing AML/CTF controls.

All Acquirers (Q2-Q4 2026)

Q2-Q4 2026: PSD3 Readiness (EU operations)

- **Merchant onboarding disclosures**: Review transparency requirements for payment accounts
- **Fee disclosure**: Assess PSD3 fee transparency and information obligations
- **Fraud prevention**: If providing payment accounts, assess verification and fraud liability provisions
- **Verification of Payee (VoP)**: Confirm ongoing compliance with VoP obligations and how these interact with any PSD3/PSR fraud-prevention changes.
- **AMLR preparation**: For EU operations, assess how the EU AML Regulation will overlay existing AML/CTF controls and any implications of EU-level supervision.

Q3 2026: Operational Resilience

- **Review incident reporting obligations** (jurisdiction-specific)
- **Assess CTP designation risk** (if systemically important UK acquirer)

6.4 Resource Requirements

6.4.1Model A (Bank-Licensed, no safeguarding)

For bank-licensed acquirers, incremental effort is primarily legal and operational: confirming that settlement flows do not create safeguarding obligations and validating that operational resilience and AI governance frameworks already meet expectations. In most cases this can be handled within existing bank change and risk teams, with a short scoping exercise rather than a dedicated safeguarding project.

6.4.2 Model B (PI, no fund holding)

Payment-institution acquirers that do not hold merchant funds typically face a modest uplift: legal scoping to confirm "no holding" status, and any PSD3-related work on fraud prevention and transparency for EU operations. Workloads will sit with compliance, legal, and product/operations teams, and can usually be integrated into broader PSD3 or operational resilience programmes rather than run as a standalone initiative.

6.4.3 Model B (PI, with fund holding)

Where PI acquirers do hold merchant funds (suspense accounts, rolling reserves, split payments), safeguarding becomes a materially larger piece of work, particularly for UK CASS 15 implementation. Firms should expect a structured project touching legal (classification and contracts), finance/treasury (account structures), operations (reconciliations), technology (data and MI), and compliance/audit (resolution packs, governance).

6.4.4 Model C (EMI-Licensed)

EMI-licensed acquirers face the highest safeguarding effort, as 100% of merchant e-money must be protected under CASS 15 in the UK and, later, PSD3 in the EU. Resource needs span programme management, treasury, operations, technology, and senior governance, with a need to design scalable daily reconciliation, multi-bank structures, and clear documentation that can support both audits and potential wind-down scenarios.



6.5 Out of Scope for Acquirers

What acquirers do NOT need to worry about:

APP Fraud Reimbursement

Why most acquirers not affected: APP fraud liability (Faster Payments / CHAPS) applies to participant banks, not acquirers (unless also operating as bank). One exception remains, and this is if the acquirer is also the sending PSP for UK Faster Payments/CHAPS (for example, because it provides payment accounts to merchants or routes settlement through its own customer accounts).

EU PSD2/EMD2/PSD3/PSR Safeguarding (UK-only acquirers)

Acquirers that operate only in the UK and do not provide EU-facing payment services or payment accounts do not need to worry about EU PSD3/PSR safeguarding or fraud-prevention obligations; their focus is on UK CASS 15 (if they hold merchant funds) and UK operational resilience.

6.6 Risk Factors & Mitigation

Regulatory Risks

RISK	MITIGATION
Misclassifying business model (treating fund-holding as pass-through) or changing it (e.g. adding rolling reserves) without revisiting scope.	Early legal scoping, documented fund flows, and mandatory legal review for model changes.
AML / merchant risk: High-risk or fraudulent merchants using acquiring flows for money laundering, sanctions breaches, or first-party fraud	Strengthen merchant onboarding and ongoing monitoring (enhanced due diligence for high-risk sectors, MCC and country controls, transaction pattern analysis, and periodic portfolio reviews).
PSD3 requirements unclear; firms over-invest in non-applicable areas	Monitor EBA technical standards, participate in industry working groups, build flexibility into systems.
Expanded APP and PSD3/PSR fraud liability where the acquirer is the sending PSP or provides payment accounts	Align fraud controls with reimbursement rules, strengthen SCA and monitoring, and clarify liability in contracts.

Operational Risks

RISK	MITIGATION
CASS 15 implementation delays; failure to be compliant from 7 May 2026 (Models B with fund holding and C)	Start design early, allocate clear ownership, involve auditors pre-go-live, third-party vendor support.
Major IT or critical third-party outages breaching UK operational resilience and EU DORA/ICT expectations	Map critical services, test impact tolerances, strengthen third-party oversight and incident response in line with UK operational resilience and DORA requirements.
Acting as safeguarding bank for PI/EMI clients without CASS 15-aligned structures (primarily Model A banks)	Review safeguarding account setups and processes and align reconciliations and incident procedures with client firms.

Reputational Risks

RISK	MITIGATION
Publicised AML/sanctions or merchant fraud failures damaging trust in the acquirer.	Demonstrate strong AML and merchant-risk controls to key merchants and partners and ensure clear incident communications where issues arise.

6.7 Key Takeaways

For acquirers, the decisive question is not what licence you hold but whether you sit on merchant money at the end of the business day. If you can evidence true pass-through with no end-of-day balances, safeguarding stays someone else's workout and your main concerns are fraud, resilience and getting your fund-flow diagrams past legal with a straight face. The moment you introduce suspense accounts, rolling reserves or e-money balances, you have quietly enrolled in the full safeguarding regime, and the regulator will expect a programme, not a policy.

Bank-licensed acquirers live in the familiar world of prudential rules, APP fraud and operational resilience, with only limited extra pain from CASS 15 or PSD3 so long as they avoid acting like PIs or EMIs in disguise.

PI acquirers get to choose their own adventure: stay lean with same-day settlement and treat safeguarding as a scoping exercise or monetise fund-holding features and accept a heavier change agenda to prove every pound is protected.

EMI acquirers, finally, trade simplicity for trust, carrying the full 100% safeguarding burden in return for a "safe-hands" positioning that will matter more once PSD3, AI governance and operational resilience expectations all converge on the same balance sheet.



Chapter 7: Banks (ASPSPs)

Introduction

This chapter is for the banks that run the rails. It pulls together what UK and EU ASPSPs must do on fraud prevention, open banking, customer protection and operational resilience, and when those obligations actually bite. In this context "banks" means deposit taking ASPSPs that provide payment accounts and access to Faster Payments, CHAPS or EU credit transfers.

IN-SCOPE FIRMS	OUT OF SCOPE
• UK-authorised banks (including building societies, credit unions with banking license) • EU-authorised banks • Banks acting as ASPSPs (providing payment accounts and access to PISPs/AISPs) • Banks acting as safeguarding banks (holding PI/EMI customer funds)	• BNPL products offered by banks (covered under consumer credit rules, not payment services) • Standalone crypto custody (covered under crypto regimes, not payment services) • Investment banks and non-deposit taking institutions (different prudential framework)

7.1 Regulatory Requirements Comparison Tables

7.1.1 UK banks: regulatory requirements (current and near-term)

Requirements

Use this table as a quick index of which UK regimes actually bite banks in 2026-2027; detailed scope, obligations and Board implications are set out in section 7.2.

REGULATORY REQUIREMENT	UK BANKS (2026-2027)	STATUS
Confirmation of Payee (CoP)	✅ CoP required on relevant FPS/CHAPS payments	Live since Oct 2024 for FPS/CHAPS participants
APP Fraud Reimbursement (Faster Payments)	✅ Mandatory reimbursement up to claim cap	Live since Oct 2024 (consumers/SMEs/charities)
APP Fraud Reimbursement (CHAPS)	✅ Mandatory reimbursement up to claim cap	Live since Oct 2024 for CHAPS participants
UK safeguarding - bank role for PIs/EMIs (CASS 15)	✅ Significant duty when acting as safeguarding bank	From 7 May 2026 where acting as safeguarding bank
UK Money Laundering Regulations (MLRs) - 2024 Amendments	✅ Mandatory AML updates	Q1 2026 - 21 days post-laying (no transition)
Open-banking API access (UK regime)	⚠️ Conditional - UK open-banking perimeter and FCA thresholds	Ongoing for in-scope ASPSPs with payment accounts
Consumer Duty (payments and fraud)	✅ Duty applies across retail/SME payment journeys	In force since July 2023 (retail/SME payment journeys)
Operational Resilience - Reporting & Incident Management	✅ UK operational-resilience obligations	Ongoing for firms in scope of FCA/PRA/BoE rules
Critical Third Party (CTP) Cooperation	⚠️ Conditional (depends on size, volume or services) and where providers are designated CTPs	From 2026 where designated CTPs are relied on
AI Governance & Explainability	✅ AI use in credit, fraud and AML	FCA guidance expected around Dec 2026 for AI in credit, fraud and AML

Legend: ✅ Applies, mandatory in principle ⚠️ Conditional (depends on size, volume or services) ❌ Not applicable or covered elsewhere

Implications

For UK banks, the 2026-2027 load is concentrated in APP fraud and CoP, safeguarding-bank duties under CASS 15, refreshed AML under the 2024 MLR amendments, and emerging AI governance expectations on top of Consumer Duty; smaller banks will absorb most of this into existing fraud, AML and resilience programmes, while larger and systemic firms will need coordinated change portfolios.

For UK banks, these are the same high-impact items that sit in the red and amber bands of the Executive Dashboard; this table is the bank-specific reading list for that page.

Note: Core prudential capital and liquidity requirements, and FSCS deposit-protection arrangements, continue to apply in full but are not listed here, as they do not introduce new 2026-2027 implementation milestones for banks.

7.1.2 EU banks: regulatory requirements (current and near-term)

Use this table as a quick index of which EU regimes actually bite banks in 2026-2027; detailed scope, obligations and Board implications are set out in section 7.3.

Requirements

REGULATORY REQUIREMENT	EU BANKS (2026-2027)	STATUS
Verification of Payee (VoP)	✅ VoP required on credit transfers in scope of Instant Payments rules	Live since 9 Oct 2025 for credit transfers
PSD3 spoofing liability & fraud prevention	✅ PSD3 fraud-prevention and spoofing-liability obligations	From late 2027 after 2026 adoption and transition
PSD3 open-banking access (APIs, NFC/FRAND)	✅ Strengthened PSD3 open-banking access obligations	From late 2027-2028 for PSD3-in-scope payment accounts
PSD3 consumer protection & spending limits	✅ PSD3 consumer-protection and spending-limit obligations	From late 2027-2028 for consumer payment accounts
Operational resilience & DORA/ICT rules	⚠️ EU operational-resilience / ICT risk obligations	Ongoing; further build-out through 2027-2028 for in-scope firms
EU Anti-Money Laundering Regulation (AMLR)	✅ New EU-level AML obligations	Applies from 10 July 2027 (EU-level AML layer)
EU AI Act - high-risk AI in financial services	✅ High-risk AI governance obligations	Applies from Dec 2027 for AI in credit, fraud and AML
Safeguarding under EMD2/PSD2/PSD3 (for banking groups with PI/EMI roles)	⚠️ Safeguarding obligations where bank group also acts as PI/EMI	PSD3 safeguarding from late 2027-2028 for in-scope PI/EMI activity

Legend: ✅ Applies, mandatory in principle ⚠️ Conditional (depends on size, volume or services) ❌ Not applicable or covered elsewhere

Implications

For EU banks, the real step-up comes from PSD3, AMLR, DORA and the EU AI Act. Together they tighten expectations on fraud, open-banking access, AML, operational resilience and AI governance, with VoP, spoofing liability, stronger open-banking obligations, EU-level AML supervision, ICT-risk requirements and high-risk AI rules all in scope. Because these changes land over broadly the same period, Boards need to treat them as a single, coordinated change agenda rather than a loose collection of parallel projects.

The regimes and dates here are exactly the same ones flagged in the Executive Dashboard heat map and timeline; this section simply shows what that cross-industry picture looks like when you sit in a bank ExCo or Board seat.

Note: CRD/CRR prudential rules and national deposit-guarantee schemes (DGS) remain fully in force across EU banks and are not shown in this index, as they do not add new 2026-2027 implementation milestones alongside PSD3, AMLR, DORA and the EU AI Act.

7.1.3 What 2026-2027 really means for banks

The UK and EU tables above are the cross-section; this is the story they tell if you sit on a bank ExCo or Board. In both jurisdictions, the 2026-2028 period brings structurally higher spend on fraud, safeguarding, AML, open banking and operational resilience, but with different main drivers: APP reimbursement, CASS 15 safeguarding-bank duties, open-banking expectations and emerging AI guidance in the UK; PSD3, VoP, AMLR and DORA-style ICT rules in the EU.

From around 2027 onwards you are dealing with the same underlying risks on both sides of the Channel, but under materially different fraud and safeguarding frameworks (PSD3/VoP/AMLR/AI Act in the EU; CASS 15/APP/Consumer Duty/UK AI guidance in the UK), so cross-border groups need one integrated bank-wide change portfolio rather than two disconnected regional projects.

In plain English:

- CoP and APP reimbursement turn Faster Payments and CHAPS into shared-liability rails for retail and SME scams, with your CoP design and fraud controls under the microscope.
- CASS 15 makes your safeguarding-bank role a regulated service from 7 May 2026, not just a convenient way to park PI/EMI client money.
- UK MLR amendments and, in the EU, AMLR push AML and sanctions expectations higher at exactly the same time as spoofing fraud and VoP tighten the fraud bar.
- PSD3, VoP and open-banking API rules turn your payment-account APIs into regulated infrastructure, not a side project for the innovation team.
- AI guidance (UK) and the EU AI Act will land squarely on the fraud, AML and credit models you already use, not on a separate “AI lab” island.

The rest of this chapter simply unpacks that agenda for UK and EU banks: same five or six themes as the Executive Dashboard, seen through a bank balance sheet and operations lens.

7.2 UK: Fraud, safeguarding-bank role and resilience

This section covers the three big pressure points for UK banks in 2026-2027: CoP and APP reimbursement on Faster Payments and CHAPS, your role as a safeguarding bank under CASS 15, and the way those sit on top of AML, operational-resilience and emerging AI-governance expectations. Together, they are one problem: how you run payments rails that are safe, resilient and explainable at scale, not three separate policy notes.

Effective Dates & Current Status: October 2024 onwards

IN-SCOPE FIRMS
• All UK-authorised banks (including building societies, credit unions with banking license) • Faster Payments participants (direct and indirect) • CHAPS participants (direct and indirect) • Banks holding safeguarded funds for PIs/EMIs (as from 7 May 2026)

7.2.1 Confirmation of Payee (CoP)

Requirement (Mandatory for most UK PSPs since October 2024):

CoP is a bank account name-checking service, designed primarily to reduce APP fraud in Faster Payments and CHAPS. It is now part of the basic plumbing for UK banks: a live fraud-control obligation, not an optional UX feature. It requires banks to check the payee name against the account name before executing relevant payments and to surface the result clearly to the customer.

IN-SCOPE FIRMS	IN-SCOPE PAYMENTS
All direct and indirect Faster Payments and CHAPS participants.	Outbound customer-initiated Faster Payments and CHAPS payments covered by the PSR's APP regime.

Main CoP requirements.

CoP ELEMENT	REQUIREMENTS	NOTES
CoP check	Compare payee name against the account name on record for in-scope FPS/CHAPS payment before execution.	Applies to both direct and indirect participants.
Response	Return a clear response: match, partial match, no match, or unavailable.	Matching logic must handle common variations (initials, abbreviations, foreign characters) without excessive false positives.
Customer warning	Present "no match" or "partial match" warnings prominently before the customer confirms the payment.	Warnings must not be buried in fine print or low-visibility screens.
Execution rules	Allow the customer to proceed, amend, or cancel after seeing the CoP result, in line with scheme rules and your risk appetite.	CoP is a warning and control; the customer always decides whether to proceed, amend, or cancel.

Liability and conduct implications:

- If a CoP check is not performed where it should have been, the bank has breached its obligations and may face both conduct risk and higher APP reimbursement exposure.
- Clear, timely CoP warnings form a key part of the "consumer standard of caution" assessment in APP cases; weak implementation makes it harder for a bank to rely on that standard.

7.2.2 APP Fraud Reimbursement (Faster Payments & CHAPS)

Requirement (Mandatory since 7 October 2024)

The UK APP fraud regime turns Faster Payments and CHAPS into shared-liability rails: both sending and receiving PSPs now fund reimbursements for qualifying victims up to a claim-level cap. CoP and APP reimbursement are designed to work together: clear "no match"-style warnings support a firm's case on reasonable caution, but ignoring a warning does not automatically remove reimbursement rights, and weak or missing CoP checks will count against the firm in PSR or FOS assessments.

PAYMENT SCOPE	Faster Payments and CHAPS payments that fall within the PSR APP reimbursement regime.
PARTICIPANT SCOPE	Both direct and indirect participants in Faster Payments and CHAPS.
VICTIM SCOPE	Consumers, small businesses, and small charities.
FRAUD SCOPE	most APP scam types, including investment scams, purchase scams, romance scams, invoice and mandate scams, and impersonation scams (for example fake bank, police or HMRC calls).
REIMBURSEMENT SCOPE	Reimbursement applies to fraud victims who are not acting fraudulently or with gross negligence.

Reimbursement rules

CIRCUMSTANCE	REIMBURSEMENT REQUIREMENT	NOTES
Qualifying APP fraud claim (in-scope customer)	Sending PSP reimburses customer up to £85,000 per claim; reimbursable loss then split 50/50 between sending and receiving PSPs.	In-scope customers: consumers, small businesses, small charities. Cap is per claim; firms may pay more voluntarily.
Sending PSP performed CoP and showed a clear "no match" warning	Customer is still in scope for reimbursement unless the PSP can evidence fraud or gross negligence.	A clearly ignored warning is one factor in applying the consumer standard of caution; it does not, on its own, remove the duty to reimburse.
Sending PSP did not perform CoP, or CoP warning not shown clearly	Eligible victim still reimbursed (up to £85,000); CoP failure does not remove sending PSP's duty.	A CoP failure is a conduct/supervisory issue for the sender, not a way to shift loss to the customer or receiving PSP.
Sending PSP applies claim excess	Sending PSP may deduct up to £100 per claim; no excess for vulnerable customers.	Waived excess cannot be recovered from the receiving PSP.
PSP relies on "consumer standard of caution"	Reimbursement can be declined only where PSP evidences customer fraud or gross negligence.	PSP bears burden of proof; CoP warnings, adherence to guidance and vulnerability are key factors.
Receiving PSP's share of loss	Receiving PSP funds 50% of reimbursed amount via FPS/CHAPS scheme settlement (bank or non-bank).	Customer always claims against sending PSP; PSP-to-PSP settlement is behind the scenes.

Operational impact

- Process fraud reports within 10 business days (acknowledgement)
- Investigate within 28 calendar days (resolution or continuation plan)
- Dispute with counterparty bank within agreed timelines
- Maintain documentation of all CoP checks performed
- Monitor for fraud indicators (velocity, velocity/amount, geographic inconsistency, etc.)

Over 2026-2027, the way you use analytics and AI in these processes will increasingly be judged alongside the outcomes: APP reimbursement, Consumer Duty and forthcoming FCA AI guidance are all talking about the same models, not three different systems.

Financial impact:

- Between 7 October 2024 and 30 September 2025, firms reimbursed around £173 million to APP scam victims, with roughly 88% of in-scope losses returned under the PSR regime[16].
- Reimbursement costs are material and concentrated in high-volume banks; better fraud controls reduce, but do not eliminate, the burden.

7.2.3 Operational Resilience Reporting & Incident Management

Requirement (Mandatory, ongoing)

UK banks must be able to keep "important business services" within impact tolerances and report material incidents to regulators on time. Operational resilience is now a standing obligation, not a one-off programme.

IN-SCOPE FIRMS	IN-SCOPE SERVICES	LIKELY REPORTABLE INCIDENTS*
Systemically important UK banks and other firms captured by the FCA/PRA/BoE operational resilience rules as defined in PS21/3 and SS1/21.	Payments processing, Faster Payments and CHAPS access, card authorisation, and other services you have mapped as "important".	• Payment system outages (for example, FPS/CHAPS or card processing disruption). • Major IT failures or critical third-party outages (cloud, processors, network providers). • Cyber and security incidents (ransomware, DDoS, data breaches) with customer or service impact. • Other events that push an important business service outside its stated impact tolerance.

** Subject to threshold tests and firm-specific impact tolerances*

Reporting expectations

While precise timelines depend on the rulebook and severity, the core pattern is:

STEP	WHAT REGULATORS EXPECT	EXAMPLE TIMING
Initial notification	Tell the FCA/PRA/BoE promptly that an important business service has suffered a major incident, including basic facts and estimated impact.	Typically within one business day.
Incident report	Provide fuller detail on root cause, customer impact, and interim mitigations.	Around five business days, or as agreed with supervisors.
Root-cause and remediation	Deliver a root-cause analysis and a credible remediation plan where the incident reveals weaknesses in controls, capacity, or third-party oversight.	Around 30 calendar days, or on a timetable agreed with the FCA/PRA/BoE.

Governance and accountability

- A named senior manager, typically in operations or risk, is personally accountable under the FCA and PRA operational resilience framework[17] [18] and the Senior Managers and Certification Regime (SMCR) for overall resilience, including incident response quality and follow-through.
- Boards and ExCos are expected to see regular MI on important business services, impact tolerances, and significant incidents, not just ad-hoc reports after failures.

What banks need in practice

- A current mapping of important business services, their supporting systems and third parties, and clearly set impact tolerances.
- A tested incident-response playbook that covers internal escalation, customer communications, and regulatory notifications.
- The ability to evidence lessons learned and control enhancements after each major incident.

7.2.4 Role as Safeguarding Bank (for PIs/EMIs)

New requirement (effective 7 May 2026, as CASS 15 go-live)

Banks that hold safeguarded funds for PIs and EMIs must support those firms' CASS 15 obligations and manage their own risk from this role. This is no longer "just another client account"; it is a regulated safeguarding relationship with explicit duties.

IN-SCOPE FIRMS	IN-SCOPE FUNDS
UK banks (including building societies and credit unions) designated by PIs/EMIs as safeguarding banks.	PI "relevant funds" and EMI e-money balances that must be safeguarded under CASS 15.

Banks' obligations as safeguarding banks

OBLIGATION	WHAT IT MEANS IN PRACTICE	WHY IT MATTERS
Segregated accounts	Provide clearly labelled safeguarding accounts, kept separate from the bank's own funds and from non-safeguarded customer money.	Supports the client PI/EMI's CASS 15 segregation and reduces commingling risk.
Daily balance support	Provide reliable daily balance information to enable the PI/EMI to perform daily internal and external reconciliations.	Without timely balances, the PI/EMI cannot meet CASS 15 daily reconciliation requirements.
Written acknowledgement	Issue written confirmations that the accounts are safeguarding accounts, that funds are held for PI/EMI customers, and that the bank has no right of set-off over those balances.	Forms part of the PI/EMI's CASS 15 evidence and clarifies the legal position in an insolvency.
No set-off / netting	Ensure internal systems and documentation do not allow set-off or netting of safeguarded balances against other exposures to the PI/EMI.	Prevents safeguarded funds being depleted to cover the PI/EMI's own debts to the bank.
Audit and access	Co-operate with the PI/EMI's safeguarding auditor and provide the information needed to verify balances and account status.	Audit evidence is now a core part of the PI/EMI's annual safeguarding opinion under CASS 15.

Banks should expect PIs and EMIs to run initial and ongoing due diligence on them as safeguarding counterparties, covering credit strength, operational resilience, and service quality.

Liability and risk implications

- If a safeguarding bank fails and safeguarded funds have been commingled or mis-segregated, customers may suffer losses and the bank's insolvency practitioners will face complex claims. FSCS does not cover PI/EMI customer funds.
- Acting as a safeguarding bank therefore creates both operational and legal risk for the bank; pricing, contractual terms and risk appetite should reflect that.
- Banks must maintain insurance or capital buffers to cover safeguarding liability.

Strategic implications

- Over time, particularly after PSD3 introduces central bank safeguarding options in the EU, some larger PIs and EMIs may move part of their safeguarded balances away from commercial banks.
- UK banks that want to retain safeguarding flows will need to offer reliable, well-documented safeguarding services and integrate them into their wider operational resilience and treasury frameworks, not treat them as generic client accounts.

7.2.5 Open Banking API Access (PISPs/AISPs)

Requirement (Ongoing, with further guidance expected)

UK banks must not obstruct PISP and AISP access to payment accounts via open banking APIs and must treat those journeys consistently with their own channels under the FCA's Consumer Duty and open banking expectations. Weak APIs or deliberate obstacles are now a conduct and supervisory issue, not just a technical nuisance.

IN-SCOPE FIRMS	IN-SCOPE FUNDS	OUT OF SCOPE
UK banks and building societies that provide payment accounts within the UK open banking regime.	API access for payment initiation and account information services on in-scope payment accounts, including consented data sharing and payment initiation via PISPs and AISPs.	UK banks that do not offer payment accounts within the open banking regime (e.g. specialist wholesale banks with no retail or SME payment accounts exposed to PISPs/AISPs).

Banks open banking obligations at a glance

OBLIGATION	WHAT IT MEANS IN PRACTICE	EXAMPLES
Access and non-discrimination	Reliable, non-discriminatory PISP/AISP access, with availability and latency broadly in line with the bank's own mobile and online channels.	API availability around 99.5% and sub-second average response times, similar to the mobile app.[19].
Documentation and support	Clear, current technical documentation and onboarding support so third parties can connect, test and go live.	Machine-readable OpenAPI specs, test data and a developer support contact.
Fraud and security controls	Proportionate fraud and security controls that manage risk without unnecessary blocking or de-facto "de-banking" of legitimate open-banking users.	Re-using existing SCA flows and thresholds instead of adding extra steps only for open-banking payments.
Pricing and throttling	Pricing, rate-limiting and other levers do not disadvantage PISPs/AISPs versus the bank's own interfaces for equivalent access.	No higher base fees or tighter call limits for standard open-banking access than for equivalent internal API use.
Legitimate differentiation	Different commercial terms only for genuinely different services and counterparties, not to sidestep open-banking duties or penalise PISPs/AISPs.	Separate pricing for cash-management APIs for large corporates, white-label products, or card-scheme interfaces outside the open-banking perimeter.
Fallback access	Where not exempt, a fallback interface is available when the dedicated API does not meet required standards.	Allowing access via a compliant modified customer interface during dedicated-API outages or persistent under-performance.
Incidents and outages	Incident handling for open-banking access meets at least the standard of the bank's own online and mobile channels.	Real-time monitoring, status updates during incidents, and post-incident fixes that include open-banking APIs.

Supervisory expectations

- The FCA, PSR, CMA and the future open-banking oversight entity monitor open-banking availability and performance and can escalate persistent weaknesses through supervisory challenge or enforcement.
- Banks should assume that sustained under-performance or unjustified friction for PISPs and AISPs is now a conduct issue, not just a technical defect.

7.2.6 Consumer Duty (payments and fraud)

Requirement (ongoing since July 2023)

UK banks must meet the FCA's Consumer Duty across all in-scope payment and fraud journeys, including Faster Payments and CHAPS, open-banking access, and card and account channels. Weak outcomes on fraud prevention, reimbursement or communications are now a conduct issue, not just a narrow rules-breach question.

IN-SCOPE FIRMS	IN-SCOPE SERVICES	OUT OF SCOPE
UK banks and building societies subject to Consumer Duty and providing payment accounts or payment services to retail and SME customers.	Faster Payments and CHAPS journeys (including APP fraud and CoP), card and account-based payments, open-banking PISP/AISP journeys on payment accounts, and related fraud-prevention, dispute and reimbursement processes.	Pure wholesale payment flows and institutional business outside Consumer Duty's retail and SME perimeter.

Consumer Duty expectations at a glance

OBLIGATION	WHAT IT MEANS IN PRACTICE	EXAMPLES
Fair value in fraud and reimbursement	Fraud controls, reimbursement policies and charges deliver fair value, not excessive loss or friction for customers.	No blanket declines on low-risk payments; APP reimbursement applied consistently; no fees that make redress meaningless.
Clear, timely communications	Customers get clear, timely fraud-related information in plain language.	Specific, prominent CoP and fraud warnings; clear letters or in-app messages explaining reimbursement decisions and any excess.
Support for vulnerable customers	Processes identify and support vulnerable customers in fraud and scam cases.	Extra help where vulnerability is flagged; tailored contact on scams; flexible evidence expectations where customers were groomed or coerced.
Proportionate fraud controls	Fraud controls reduce harm without unnecessary "de-banking" or access barriers for legitimate users and PISPs/AISPs.	Monitoring false-positive rates; adjusting rules that hit certain segments unfairly; avoiding systematic blocking of PISP-originated payments without proven risk.
Outcome monitoring and MI	Outcomes across payment and fraud journeys are monitored and used to improve results, not just loss ratios.	MI on fraud incidence, reimbursement rates, complaints, vulnerable-customer outcomes and CoP warning effectiveness reported to ExCo/Board.
Governance and accountability	Senior management and the Board own Consumer Duty outcomes for payments and fraud.	Clear SMCR allocation; Consumer Duty reviews covering CoP, APP reimbursement, open-banking access and card disputes together.

Supervisory expectations

- The FCA increasingly assesses APP reimbursement, open-banking access and fraud-control design through a Consumer Duty lens, not just against individual rules.
- Banks should assume that patterns such as systematic non-reimbursement of scam victims, persistent "de-banking" via over-zealous fraud controls, or opaque communications on fraud decisions may be treated as Consumer Duty failings even where narrow rule compliance is arguable.

7.2.7 UK Money Laundering Regulations (MLRs) - 2024 Amendments

New requirement (Q1 2026, 21 days post-laying)

UK banks must implement the 2024 amendments to the UK Money Laundering Regulations, which introduce enhanced AML expectations that apply immediately once the amending instrument is laid, with no transition period.

IN-SCOPE FIRMS	IN-SCOPE SERVICES
All UK-authorised banks and building societies, and other UK financial institutions subject to the MLRs.	All in-scope banking and financial services covered by the UK MLRs, including retail, SME and wholesale business.

Expected obligations

OBLIGATION	WHAT IT MEANS IN PRACTICE	EXAMPLES
Enhanced customer due diligence (CDD) for higher-risk customers	Apply deeper, more frequent CDD and ongoing monitoring where customer, product, geography or delivery channel indicators point to higher ML/TF risk.	Additional source-of-funds and source-of-wealth checks for higher-risk customers; more frequent KYC refresh for certain sectors or jurisdictions.
More granular beneficial-ownership verification	Strengthen the way beneficial owners are identified and verified, using improved data sources and more robust cross-checks.	Cross-checking company-register data against independent data sources; using enhanced tools, including any piloted blockchain-based verification solutions where appropriate.
Sanctions-screening enhancements	Increase the frequency, coverage and quality of sanctions-screening, and tighten alert handling and escalation.	More frequent list updates; expanded geographic coverage; clearer SLAs for alert review and escalation to sanctions specialists.
Cryptocurrency-related transaction monitoring	Improve detection and investigation of higher-risk crypto-linked transactions where the bank has exposure to exchange-to-wallet or similar flows.	Flagging and reviewing customer payments to and from known exchanges or wallets where risk indicators are present; updating typologies and scenarios in transaction-monitoring systems.

Strategic implications

- The 2024 MLR amendments turn AML into an integral part of the 2026-2027 change agenda for banks, alongside APP fraud reimbursement, safeguarding-bank duties and open-banking/AI work, rather than a separate compliance track.
- Higher-risk customer segments, complex ownership structures and crypto-exposed flows will attract more supervisory attention, so firms that cannot evidence strong CDD, ownership checks and sanctions controls in these areas should expect challenge.
- For groups with EU banks, UK MLR work needs to be planned in parallel with EU AMLR preparation so that AML governance, data and monitoring evolve towards a single, coherent framework rather than diverging by region.

7.3 EU: PSD3, VoP, AMLR and AI Act

Effective Dates & Current Status: October 2025 onwards, with PSD3 transition in Q4 2027

IN-SCOPE FIRMS
• All EU-authorised banks • Verification of Payee (VoP): All banks executing credit transfers • PSD3: All banks (post-adoption and implementation, estimated Q4 2027)

7.3.1 Verification of Payee (VoP)

Requirement (Mandatory since 9 October 2025)

EU banks must apply Verification of Payee checks on in-scope credit transfers, comparing the beneficiary name provided by the payer with the account holder name and acting on the result in line with Instant Payments Regulation requirements and forthcoming EBA standards.

IN-SCOPE FIRMS	IN-SCOPE PAYMENTS
All EU-authorised banks executing credit transfers within the scope of the Instant Payments Regulation.	Outbound credit transfers (domestic and cross-border) that fall under the Instant Payments rules, including instant and non-instant euro credit transfers where VoP is mandated.

Main VoP requirements

VoP ELEMENT	REQUIREMENTS	WHAT THIS MEANS IN PRACTICE
VoP name check	Compare the beneficiary name entered by the customer with the account-holder name on record before executing an in-scope credit transfer.	Use matching logic that tolerates common variations (initials, minor spelling differences) but flags genuine mismatches.
Response categories	Return a VoP result for each in-scope payment: match, close match, no match, or unavailable (for example where the payee bank cannot provide data).	"Match" or "close match" can proceed normally; "no match" or "unavailable" require an additional step.
Customer warning and consent	Where VoP returns "no match", warn the customer clearly and require explicit confirmation before executing; firms may decline in very high-risk cases.	Present a prominent on-screen warning and require the customer to confirm they still wish to proceed before sending.
Cross-border handling	Implement VoP for cross-border credit transfers where counterparties participate; handle "unavailable" results where foreign banks cannot yet supply data.	Where VoP is unavailable, warn the customer and apply enhanced monitoring or other controls based on risk appetite.

Differences from UK CoP

- VoP applies to all in-scope credit transfers rather than only Faster Payments and CHAPS-equivalent rails.
- Execution rules are more prescriptive: "no match" requires explicit customer consent to proceed and may justify refusal in high-risk cases, rather than operating purely as a warning.
- VoP covers cross-border transfers within its scope, increasing operational complexity compared with the UK's largely domestic CoP focus.

Strategic implications

- VoP turns name-checking into a core control for all in-scope EU credit transfers, not just instant payments, which means banks need robust matching logic, customer-communication journeys and exception handling baked into their payment platforms.
- The cross-border element and stricter execution rules raise the bar for AML and fraud-control integration, especially where correspondent or foreign-bank dependencies make VoP "unavailable" in some routes.

7.3.2 PSD3 Fraud Prevention & Spoofing Liability

Requirement (Estimated Q4 2027, post-adoption and implementation)

Once PSD3/PSR applies, EU banks must implement enhanced fraud-prevention controls and meet new "spoofing" liability rules for certain impersonation scams, following an 18-21 month transition period after PSD3 adoption in 2026.

IN-SCOPE FIRMS	IN-SCOPE PAYMENTS
All EU-authorised banks executing payment transactions within the scope of PSD3/PSR.	Payment transactions initiated by customers that fall under PSD3, including instant and non-instant credit transfers and other electronic payments where spoofing scenarios are relevant.

Spoofing liability and fraud-prevention expectations

OBLIGATION	REQUIREMENTS	WHAT THIS MEANS IN PRACTICE
Enhanced fraud-prevention controls	Maintain fraud-prevention measures that are demonstrably effective at detecting and stopping high-risk payments, including impersonation scams.	Strengthen scenarios, thresholds and monitoring for unusual patterns (for example new payees, high-value or unusual-destination transfers).
Spoofing liability for impersonation fraud	Reimburse customers where losses arise from specified employee or bank-impersonation frauds and the bank's controls were inadequate, with limited or no ability to rely on "gross negligence" carve-outs.	Treat qualifying spoofing cases as reimbursable unless you can evidence strong controls and clear customer failings; factor the new liability into reserves and pricing.
Reimbursement level and scope	In qualifying spoofing cases, sending banks must reimburse up to 100% of the loss and cannot rely on "gross negligence"; receiving banks may also be liable where they ignore clear suspicious indicators.	Assume full reimbursement for in-scope spoofing unless you can show the case falls outside PSD3 criteria and that both sending and receiving banks had adequate controls and escalation.
Multi-factor authentication for high-risk transactions	Apply multi-factor authentication and additional verification for high-value or high-risk transactions as part of the anti-spoofing control set.	Step-up authentication on certain payees, amounts or patterns; add extra checks before releasing payments that match spoofing typologies.
Customer-contact and verification controls	Implement stronger verification when customers receive instructions that appear to come from the bank or its staff, especially for high-risk transactions.	Encourage "call-back" via published numbers; challenge unusual instructions; warn customers against acting on unsolicited calls, emails or messages.
Internal processes and fraud-intelligence sharing	Ensure fraud teams can recognise and escalate spoofing cases and take part in industry-level sharing on new impersonation typologies.	Feed external alerts and industry intelligence into models; share data on emerging spoofing patterns through industry fraud forums where permitted.

Differences from UK APP fraud regime

- PSD3 introduces a specific spoofing liability framework for EU banks, whereas UK banks operate under the broader APP reimbursement regime for Faster Payments and CHAPS.
- The PSD3 model is expected to give less room to rely on "gross negligence" in some impersonation cases, increasing structural liability compared with current UK practice.
- EU spoofing rules will sit alongside VoP and PSD3's wider fraud-prevention expectations, creating a single, integrated fraud-liability regime for EU banks rather than the UK's mix of CoP, APP reimbursement and Consumer Duty.

Financial impact

- Spoofing liability creates a new, distinct reimbursement category for EU banks, with aggregate losses across the EU likely to be significant (industry estimates are in the hundreds of millions of euros annually).
- Liability can be higher than under some existing APP-style models because the "no gross negligence" argument is narrowed or removed for qualifying spoofing cases, making control effectiveness and evidence particularly important.

Strategic implications

- Spoofing liability will push EU banks to invest more heavily in front-to-back fraud controls, customer-contact design and staff training, and to treat impersonation scams as a core conduct and P&L issue.
- Fraud-prevention models, VoP, authentication and customer-contact journeys need to be designed as a single architecture, so that name-checking, behavioural analytics, holds and verification reinforce each other rather than operating as disconnected controls.

7.3.3 PSD3 Open Banking Access

Requirement (Estimated Q4 2027, post-adoption and implementation)

Once PSD3/PSR applies, EU banks must provide non-discriminatory access to payment accounts for PISPs and AISPs and meet new EBA technical standards on API performance and availability, following an 18-21 month transition period after PSD3 adoption in 2026.

IN-SCOPE FIRMS	IN-SCOPE SERVICES
All EU-authorised banks offering PSD3-in-scope payment accounts.	Outbound credit transfers (domestic and cross-border) that fall under the Instant Payments rules, including instant and non-instant euro credit transfers where VoP is mandated.

Main PSD3 open-banking access obligations

REQUIREMENT	REQUIREMENTS	WHAT THIS MEANS IN PRACTICE
API performance standards	Meet EBA-defined benchmarks for API uptime, response times and data quality.	Design and operate APIs with performance comparable to the bank's own channels; monitor and report availability and latency.
Removal of "security" obstacles	Do not use "security" as a pretext to impose excessive friction on PISP/AISP journeys, such as unnecessary re-authentication or throttling.	Avoid extra SCA steps or rate limits that only apply to PISP traffic; align open-banking SCA and UX with those for the bank's own digital channels for equivalent services.
Mobile OS integration	Support the opening of Apple and Google NFC and related interfaces to PISPs on FRAND terms, so that PISP-initiated mobile payments can run over bank APIs.	Prepare to work with PISPs that build their own mobile wallets and contactless journeys using NFC, Face ID and Touch ID, rather than relying only on proprietary wallets.
Real-time data access	Provide near real-time account and transaction data to PISPs/AISPs, not just batch or delayed updates.	Support continuous data feeds; minimise latency so PISP apps can show up-to-date balances and transactions.
Data portability	Enable customers to port account history and other relevant data to PISPs/AISPs on request.	Allow customers to authorise export of account history for analytics and value-added services in PISP apps.
Non-discriminatory access and pricing	Offer PISPs/AISPs access on non-discriminatory terms compared with internal or affiliated services, in line with PSD3 and FRAND-style expectations.	Do not refuse access or impose materially worse pricing or service levels on PISPs/AISPs purely because they compete with the bank's own products.
API upgrade and migration	Update APIs to comply with PSD3 technical standards within the implementation window (likely 12-18 months) and manage migration from PSD2 interfaces.	Run a structured API upgrade and deprecation programme, with clear testing windows and support for third-party developers.

Strategic implications

- PSD3 shifts open banking from a largely principles-based PSD2 duty to a more prescriptive access regime, so EU banks need to treat API quality and non-discrimination as core payments infrastructure rather than a side project.
- Stronger access rules, performance benchmarks and mobile-OS opening will increase competitive pressure from PISPs and aggregators, so banks that want to remain visible at the customer interface will need explicit API, partnership and product strategies instead of relying on friction to defend their position.
- Unlike the UK's PSD2-based regime, PSD3 will give EU PISPs and AISPs stronger, benchmarked access rights and a clearer anti-obstacle toolkit.

7.3.4 PSD3 Consumer Protection & Spending Limits

Requirement (Estimated Q4 2027, post-adoption and implementation)

Once PSD3/PSR applies, EU banks must implement consumer spending-limit and transaction-control tools for payment accounts, following the post-adoption transition period.

IN-SCOPE FIRMS	IN-SCOPE SERVICES
All EU banks offering PSD3-in-scope payment accounts to consumers.	Consumer payment-account services, including debit and credit functionality and recurring payments within PSD3 scope.

Main PSD3 open-banking access obligations

REQUIREMENT	REQUIREMENTS	WHAT THIS MEANS IN PRACTICE
Customer-set spending limits	Allow customers to set daily, weekly or monthly caps on debit and credit spending.	Add configurable spending-cap settings to digital channels.
Transaction-blocking rules	Enable customers to define rules blocking certain transaction types or destinations.	Provide simple on/off controls for categories such as international transfers.
Fraud-detection holds	Apply automatic holds for transactions that trigger fraud-risk indicators, with customer confirmation before release.	Introduce short payment holds and a confirmation step for suspicious transactions.
Payment-plan notifications	Notify customers at least a few days before recurring payments and instalments are due.	Send advance alerts ahead of scheduled debits so customers can review or cancel.

Differences from FCA Consumer Duty

- PSD3 introduces specific mandated tools (spending caps, blocking rules, fraud-hold mechanics and notifications), whereas the UK Consumer Duty remains principles-based and leaves banks more discretion in how they deliver good outcomes.
- Post-PSD3, EU banks will operate under a more standardised consumer-protection framework for payment accounts, while UK banks will continue to evidence outcomes with greater flexibility over tooling.

Strategic implications

- These controls will reset customer expectations so that configurable limits, blocking rules and alerts become standard features of EU payment accounts, meaning banks need to factor them into their core product and technology plans rather than treating them as add-ons.
- The new controls will generate richer data on customer behaviour and risk, creating opportunities for better fraud-prevention and financial-health tools, but they will also need to be aligned with privacy, AI-governance and conduct requirements.

7.3.5 EU Anti-Money Laundering Regulation (AMLR)

Requirement (Effective 10 July 2027)

From 10 July 2027, the EU Anti-Money Laundering Regulation (AMLR) will introduce a more centralised EU-level AML/CFT regime, including direct EBA/ECB supervision of certain high-risk institutions, replacing today's predominantly national-level supervisory model.

IN-SCOPE FIRMS	IN-SCOPE SERVICES
All EU banks and other in-scope financial institutions.	All AML/CFT-relevant activities, including onboarding, transaction monitoring, sanctions screening and reporting obligations.

Key AMLR changes

REQUIREMENT	REQUIREMENTS	WHAT THIS MEANS IN PRACTICE
Direct EU-level supervision	Enable the EBA/ECB to directly supervise high-risk institutions alongside national AML authorities.	Prepare for dual supervisory engagement and more intensive reviews for higher-risk groups.
Harmonised AML rules	Apply a single, directly applicable AML rulebook across EU member states.	Reduce local variations but expect less flexibility to rely on national "gold-plating" or gaps.
Beneficial-ownership transparency	Support an enhanced, EU-wide beneficial-ownership registry.	Align KYC and onboarding processes with a central EU BO database.
Crypto-asset monitoring	Follow more granular rules for monitoring cryptocurrency and exchange-to-wallet transfers.	Upgrade monitoring scenarios and data capture for crypto-related flows.
Sanctions screening	Implement near real-time sanctions-list updates (for example via the SWIFT sanctions protocol).	Tighten sanctions screening systems and processes to ingest and act on frequent updates.

Enforcement implications

- The EBA will be able to impose sanctions directly, including fines up to €5m or 2% of global revenue in serious cases.
- High-risk institutions will face dual supervision (national authority plus EU-level), increasing oversight intensity and compliance burden.

Strategic implications

- AMLR shifts AML/CFT from a largely national rule-interpretation exercise to a more uniform, EU-level regime, so groups operating across multiple member states will need to converge policies, systems and controls onto a single EU standard.
- Direct EU supervision and higher expectations on sanctions, BO data and crypto monitoring will raise the bar for analytics, data quality and model governance, making AML/CFT capabilities a board-level infrastructure topic rather than a back-office compliance task.

7.4 Priority Action Timeline

UK banks (Q1 2026-Q4 2027 & Beyond)

CRITICAL (Already Effective - Ongoing compliance)

- CoP and APP fraud reimbursement (since October 2024)
- Operational resilience and incident management

IMMEDIATE Q1 2026	Q3 2026 Design & Preparation	Q4 2026 Embedding & external engagement	2027 & Beyond Horizon items
• **UK MLR 2024 amendments** - implement updated CDD/EDD, BO checks, sanctions and monitoring 21 days post-laying • **Safeguarding-bank readiness for CASS 15 -** segregated safeguarding accounts, no set-off, daily balances, written acknowledgements by 7 May 2026	• **AI governance groundwork -** build a single model inventory and governance approach for fraud, credit and AML models that already run your CoP/APP, MLR and credit-decisioning stack ahead of FCA AI guidance • **APP fraud review preparation -** assess potential PSR changes to reimbursement caps, excesses and evidence standards	• **Implement any APP fraud review outcomes -** adjust controls, policies, MI and customer journeys • **Engage on National Payments Vision -** respond to Pay.UK and align internal payment-platform plans so your FPS/CHAPS and account-to-account upgrades also make it cheaper to deliver CoP/APP, PSD3-style access, AMLR and AI-governance expectations on those rails.	• **Critical Third Party (CTP) regime -** identify key providers and align third-party risk and incident processes • **Operational resilience enhancements** • **Post-quantum cryptography -** track standards and start scoping migration for payments and core banking

EU Banks (Q1 2026-Q4 2027)

CRITICAL (Already Effective - Ongoing compliance)

- Verification of Payee (VoP) - apply to in-scope credit transfers under Instant Payments Regulation)
- DORA/ICT risk and existing AML - maintain ICT and AML controls at current EU/national standards

Q2 2026 Post-PSD3 adoption assessment	Q4 2026 - Q2 2027 Implementation Planning	10 JULY 2027 AMLR Go Live	Q4 2027 & Beyond Horizon items
• **PSD3/PSR gap analysis** - assess impacts on spoofing liability, SCA, open-banking APIs, consumer payment account tools and group PI/EMI safeguarding • **EBA technical-standards monitoring** - track PSD3 RTS/ITS and map affected systems • **AMLR target-model design** - define group-wide AMLR operating model	• **PSD3 implementation roadmap -** plan phased delivery of fraud/SCA changes, API upgrades and consumer-account tools • **AMLR implementation programme -** finalise BO, sanctions and crypto-monitoring enhancements and MI/reporting upgrades • **EU AI Act preparation -** identify high-risk AI models (credit, fraud, AML) and design governance, explainability and bias-testing	• **Operate under AMLR** with harmonised policies, BO data, sanctions and crypto-monitoring, and prepare for dual supervision	• **From late 2027 (PSD3/PSR application)* -** begin phased implementation of PSD3 fraud, SCA, open-banking and consumer-account changes • **From December 2027 (EU AI Act) -** bring high-risk AI models into the AI Act framework and integrate with PSD3/AMLR governance • **Post-quantum cryptography** - monitor EU/NIST guidance and feed into long-term payments and core-banking plans

** Subject to national implementation and the 18-21 month transition period after PSD3/PSR adoption in 2026.*

7.5 Resource Requirements by Bank Size

Small/Regional Banks (< £50B total assets)

Smaller banks will typically absorb CoP, APP fraud reimbursement, safeguarding-bank duties, VoP, and AMLR within existing risk, compliance, and operations teams, supplemented by targeted change activity.

The main demands are enhancing fraud-detection and reimbursement processes, updating AML/CFT controls, and establishing the processes and documentation needed to act as a safeguarding bank for PIs/EMIs.

Recommended approach:

- Use established third-party solutions where possible for CoP/VoP and fraud analytics, and rely on industry guidance and working groups to interpret PSD3 and AMLR expectations.
- Focus resources on getting core processes robust (fraud reimbursement, incident reporting, safeguarding bank operations) rather than building bespoke tooling in every area.

Large Banks (£50B-£500B total assets)

Larger banks will tend to run PSD3, AMLR, CoP/VoP, APP fraud reimbursement, and safeguarding-bank changes as a portfolio of programmes, with dedicated teams in fraud, open banking, AML, and payments operations.

Scale and complexity (multiple business lines, legacy systems, cross-border operations) mean more structured programme management, data and MI work, and heavier engagement with regulators and industry bodies.

Recommended approach:

- Establish a central regulatory change function to coordinate timelines and dependencies across fraud, safeguarding, AML, open banking, and AI governance.
- Prioritise investment in data, analytics, and API platforms that can serve multiple regimes simultaneously (for example, one fraud/transaction-monitoring stack that serves CoP/APP, PSD3 spoofing, and AMLR).

Systemically Important Banks (> £500B total assets)

Systemically important institutions face the broadest and deepest set of obligations, including likely involvement in CTP frameworks, direct EU-level AML supervision, and leading roles as safeguarding banks and scheme participants.

This usually requires permanent, cross-functional regulatory change teams, extensive technology and data modernisation, and formal board-level oversight of fraud, AML, and operational resilience programmes.

Recommended approach:

- Treat PSD3, AMLR, AI governance, safeguarding, and CTP resilience as interlocking components of a long-term transformation agenda, not a sequence of isolated projects.
- Invest early in governance, architecture, and data strategies that allow new requirements to be layered onto a common platform, reducing the need for repetitive, siloed change.

7.6 Risk Factors & Mitigation

Regulatory Risks

RISK	MITIGATION
UK: CoP/APP fraud implementation below PSR expectations.	Align design with FCA/PSR and industry guidance, and maintain a clear audit trail of CoP checks, fraud decisions and reimbursements.
EU: PSD3/AMLR timing and content uncertainty	Track PSD3/PSR and EBA outputs, run post-adoption gap analysis, and phase fraud, SCA, API and AML changes as standards are finalised
Both: Expanding fraud-liability regimes outpace controls and budget.	Strengthen end-to-end fraud controls (CoP/VoP plus analytics), add step-up checks for high-risk payments, and recalibrate risk appetite and reserves regularly.

Operational Risks

RISK	MITIGATION
Both: CoP/VoP implementation defects (poor matching logic, high false positives/negatives, weak handling of "no match"/"unavailable").	Deploy proven matching tools, run extensive pre-go-live and post-go-live testing, set clear rules for "no match"/"unavailable", and monitor match-rate MI with manual-override options.
Both: Payments and open-banking API outages or latency breaching operational-resilience or ICT expectations.	Treat payment and API channels as important business services: maintain current service maps and impact tolerances, invest in resilient API infrastructure and monitoring, and operate tested incident-response and customer-communication playbooks.
UK: Safeguarding-bank role for PIs/EMIs under CASS 15 not fully operationalised by 7 May 2026 (for example set-off, balance data, acknowledgements).	Build a defined safeguarding-bank service: segregated accounts, no set-off, reliable daily balance data, written acknowledgements, and playbooks to support client audits and resolution packs.

Strategic Risks

RISK	MITIGATION
Both: Rising PSD3/open-banking benchmarks and AI expectations widen the gap between large and smaller banks' capabilities.	For smaller and regional banks, consider shared or third-party API platforms and fraud/AML utilities; for larger groups, coordinate PSD3, open-banking and AI work through a central change portfolio rather than isolated projects.
EU: Central-bank safeguarding options plus PSD3/AMLR push PI/EMI balances away from commercial banks.	Develop a safeguarding value proposition (reliability, MI, integrated services) and pricing, and plan for funding diversification if larger clients shift part of their safeguarded funds to central banks.
Both: AI-driven models in fraud and credit create unexplained outcomes or bias that breach Consumer Duty (UK) or EU AI-Act-style expectations.	Implement a cross-bank AI governance framework (model inventory, explainability, bias testing, human oversight) aligned with fraud, AML and credit-risk programmes and sized to forthcoming FCA AI guidance and the EU AI Act.

This list focuses on bank-specific failure modes. The cross-cutting risks around mis-classified fund flows, dual UK/EU portfolios and fragmented change programmes are pulled together in Chapter 9; banks should read those alongside this chapter when they set their 2026-2027 change portfolio.

Chapter 8: Card Issuers

Scope Statement

This chapter consolidates regulatory obligations for credit and debit card issuers across UK and EU jurisdictions. Card issuers face emerging obligations around AI governance, fraud prevention, and consumer protection, but unlike payment institutions, most card issuers are NOT subject to safeguarding obligations (funds subject to bank capital requirements or card scheme rules). This chapter focuses on statutory and regulatory obligations (for example PSD3/PSR, Consumer Duty, AI governance, fraud, and AML). Card scheme rules (such as Visa and Mastercard issuing rulebooks) apply separately and continue to bind scheme-member issuers, but they are not analysed here.

Stakeholders covered:

- Banks issuing credit/debit cards (UK and EU)
- Non-bank card issuers (fintech, embedded finance)
- All card products (credit, debit, prepaid, virtual)

Out of scope:

- Card scheme governance (Visa/Mastercard rules)
- Merchant acquiring (covered in Chapter 6)
- Standalone BNPL issuers (covered in Chapter 5)

How to read this chapter:

- **If you are a bank issuer**, read this chapter on top of Chapter 7 (banks) and the AI/operational-resilience themes in Chapter 9.
- **If you are an EMI issuer**, read it on top of Chapters 1-2 (EMIs and safeguarding) and Chapter 9.
- **If you run card programmes off a PI licence or in partnership with a bank/EMI**, use this chapter for the card-specific fraud, SCA and AI points and refer back to your underlying bank or EMI chapter for stored-value and safeguarding obligations.



8.1 Regulatory Requirements Comparison Table

Legend: ✅ Applies / mandatory ⚠️ Limited / different ❌ Not applicable or alternative framework

Dimension / Requirement	UK card issuers	EU card issuers (post-PSD3 / AI Act)	What it tells you (2026-2028)
PSD3/PSR scope for issuing	❌ (UK PSRs + FCA only)	✅	UK stays on UK PSRs; EU moves to PSD3 for issuing.
Fraud liability - core model	✅ Scheme chargeback; APP only if also FPS/CHAPS sending PSP (Ch.7)	✅ Scheme chargeback + PSD3 spoofing layer	EU issuers get extra spoofing liability on top of schemes.
Strong Customer Authentication (SCA)	⚠️ PSD2-derived, FCA-guided	✅ PSD3 outcomes-based SCA	EU issuers get more SCA flexibility but more outcome scrutiny.
MOTO / MIT SCA treatment	⚠️ FCA guidance	✅ PSD3 clarifications	EU issuers get clearer MOTO/MIT rules; UK relies on guidance.
Consumer tools (spending caps, blocks, fraud holds)	⚠️ No mandated toolkit; expectations via Consumer Duty/card rules	✅ PSD3-mandated tools on consumer accounts	EU issuers must build caps/blocks/holds; UK judged on outcomes.
AI governance - credit & fraud	✅ Consumer Duty + FCA AI guidance (2026)	✅ EU AI Act high-risk AI (2027)	Both must formalise AI governance, via different regimes.
Consumer-credit conduct regime	✅ Consumer Duty + CONC	⚠️ CCD/PSD3/AI Act (no Consumer Duty)	UK issuers answer to Consumer Duty; EU to CCD/PSD3/AI Act.
Safeguarding (CASS 15 / PSD3)	⚠️ Banks: prudential + schemes (no CASS 15). EMIs: CASS 15/EMR for e-money (Ch.1-2)	⚠️ Only where group also PI/EMI (Ch.1-2)	Issuing alone doesn't trigger safeguarding; PI/EMI roles do.
APP / CoP / VoP interaction	⚠️ APP/CoP on FPS/CHAPS at bank level, not card rails (Ch.7)	⚠️ VoP/PSD3 spoofing on credit transfers, not card rails (Ch.7)	Mixed groups must join up card fraud with APP/VoP; pure issuers stay in card world.
Operational resilience	✅ Card issuing/authorisation = important business service under UK op-res (Ch.7)	✅ In-scope under ICT/DORA in banking groups	Card issuing is one "important service" in the wider resilience stack.
Cost to comply (incremental)	⚠️ AI + Consumer Duty uplift; rises with portfolio size/model complexity	⚠️ PSD3 (SCA/spoofing/tools) + AI-Act uplift; higher for large issuers	Both see rising compliance/tech cost; EU skewed to PSD3/AI Act, UK to Consumer Duty/FCA AI.

8.2 UK-Specific Requirements for Card Issuers

Effective Dates & Current Status: Ongoing

Applies to:

- All UK-authorised card issuers (banks and non-banks)
- All card products (credit, debit, prepaid, virtual)

8.2.1 FCA Consumer Duty & Credit Decisioning

Requirement (ongoing, with enhanced AI guidance expected December 2026):

Card issuers sit at the intersection of Consumer Duty, credit-decisioning rules and forthcoming FCA AI guidance: you are expected to take credit decisions that support customers' financial wellbeing, explain automated declines and limit changes in plain language, and avoid letting fraud or credit models quietly "de-bank" legitimate customers.

For issuers, the hot spots are:

- Automated application and limit-increase decisions that rely on opaque scoring models.
- "Computer says no" declines with no meaningful explanation or route to reconsideration.
- Fraud models that block large volumes of legitimate transactions for certain segments. The underlying AI governance framework (model inventory, explainability, bias testing, human oversight) should be the same one your group uses for fraud and credit models in Chapters 7 and 9; this chapter simply highlights how those expectations land on card underwriting and fraud controls.

8.2.2 Fraud Detection & De-Banking Risk

Requirement (ongoing, no new deadline but increasing scrutiny):

- Issuers must balance fraud prevention with customer access to their cards.
- FCA is concerned about effective "de-banking" of customers through overly aggressive card-fraud AI (blocking or restricting normal use of their cards).
- Compliance framework: Consumer Duty + existing fraud prevention rules.

De-banking risk context:

- Some card issuers using AI to block transactions proactively (fraud prevention).
- Risk: Legitimate customers blocked from legitimate transactions.
- FCA enforcement signal: Balance sheet freezes and account closures subject to Consumer Duty.

Mitigation strategies:

- Implement graduated response (warning → soft block → hard block).
- Maintain human override capability for edge cases.
- Clear customer communication on fraud holds (why, how long, how to appeal).
- Regular testing on false-positive rates (minimise innocent customer blocks).

Compliance implications:

- Review AI logic for fraud prevention (false-positive rates, customer impact).
- Establish appeals process for fraud-blocked transactions.
- Train fraud operations team on Consumer Duty.

For bank issuers, these expectations sit alongside the broader fraud and APP-reimbursement duties in Chapter 7.

For non-bank issuers (for example EMIs or standalone card lenders), they should be built into the same AI and outcome-testing framework you use for your other credit products and fraud controls, as described in the cross-cutting AI and operational-resilience themes in Chapter 9.

8.2.3 Operational Resilience (if systemically important)

Requirement (Ongoing):

Operational-resilience expectations for card issuing mirror those for banks in Chapter 7: issuers must treat card issuing and authorisation as important business services, map the systems and third parties that support them, and be able to keep those services within impact tolerances and report material incidents.

See 7.2.3 for the detailed playbook; do not build a separate resilience framework just for cards.

8.3 EU-Specific Requirements for Card Issuers

Effective Dates & Current Status: Q4 2027 estimated (post-PSD3 implementation)

Applies to:

- All EU-authorised card issuers
- PSD3 requirements (estimated Q4 2027 implementation)

8.3.1 PSD3 Strong Customer Authentication (SCA) - Outcomes Based

Requirement (Estimated Q4 2027, post-PSD3 adoption and implementation):

- Focus: Fraud prevention effectiveness rather than specific technical standards
- Scope: All EU card issuers executing transactions

Key differences from current PSD2 SCA:

- **Current (PSD2)**: Prescriptive 3-factor SCA (knowledge +possession + inherence)
- **Future (PSD3)**: Outcomes-based (demonstrable fraud prevention, not specific technology)

Implications for card issuers:

- 3DS not mandatory if demonstrating equivalent fraud prevention
- Multi-factor authentication frameworks (biometrics, passwordless) accepted
- Machine learning fraud detection may substitute for SCA in low-risk scenarios
- MOTO (Mail Order Telephone Order) clarifications (likely exempted from SCA for merchant-initiated payments)

Regulatory impact:

- Greater flexibility on authentication methods
- Focus shifts to fraud prevention metrics (false positives, fraud reduction rates)
- Compliance easier for issuers investing in AI fraud detection

8.3.2 PSD3 Fraud Liability & Spoofing

Requirement (Estimated Q4 2027):

- PSD3 introduces "spoofing" liability (employee impersonation fraud)
- Card issuer liable if fails to prevent fraudster impersonating card network representative
- Scope: New liability category (in addition to traditional card chargeback framework)

Spoofing fraud example:

- Fraudster calls cardholder posing as card issuer representative
- Fraudster requests one-time code or card authorisation
- Cardholder transfers funds or authorises payment
- Card issuer liable if failed to implement verification controls

Control requirements (expected under PSD3):

- Employee verification protocols (customer can call bank back on verified number)
- Transaction authorisation verification (additional step for high-value transfers)
- Fraud intelligence sharing (coordinate response to known spoofing schemes)

Financial impact:

- New reimbursement category for EU issuers
- Higher than traditional card fraud liability

Compliance implications:

- Implement employee verification protocols
- Update customer communication (fraud warning calls)
- Establish fraud intelligence sharing framework

8.3.3 PSD3 Consumer Protection & Spending Limits

Requirement (Estimated Q4 2027):

- EU cardholders can set spending limits (daily/weekly/monthly caps)
- Automatic fraud detection holds (72-hour hold for suspicious transactions)
- Cardholder consent required before payment plan deduction

Compliance implications:

- Update card systems to support granular spending limits
- Implement automated fraud holds with notification
- Clear customer communication on holds and appeals

8.3.4 EU AI Act (December 2027)

Requirement (Expected to apply from December 2027):

For EU issuers, the AI Act will treat credit-decisioning and fraud-detection models in card portfolios as high-risk AI, subject to the same governance, documentation and oversight regime described in Chapter 9. In practice you do not need a separate AI framework for cards; you need to ensure your group-wide high-risk-AI governance (model inventory, training-data and performance documentation, bias testing, human-in-the-loop oversight) explicitly covers card-issuer models as well as banking and BNPL models.

8.4 Priority Action Timeline

- Hard stop / go-live date / legal obligation starts.
- Build / implementation / preparation work.
- Long-term monitoring / horizon.

UK Card Issuers (Q1-Q4 2026)

Q1 2026 (Immediate)
Preparation and design work

- **FCA AI Governance Preparation -** Pre-December 2026.
- **Consumer Duty Review -** Q1-Q2 2026.
- **De-Banking Risk Assessment -** Q1 2026.

Q2-Q4 2026
Embedding and response

- **FCA AI Guidance Response -** around December 2026 (subject to FCA final timetable).
- **Operational Resilience Enhancement -** ongoing (if systemically important).

EU Card Issuers (Q1 2026-Q4 2027)

Q2 2026
PSD3 prep post-adoption

- **PSD3 Gap Analysis** - Post-adoption (Q2 2026).
- **EBA Technical Standards Monitoring** - ongoing (Q2 2026+).

Q4 2026-Q2 2027
Implementation Planning

- **SCA System Roadmap -** Q4 2026 onwards.
- **Spoofing Liability Preparation -** Q4 2026 onwards.
- **EU AI Act Preparation -** Q4 2026 onwards.

Q3 2027-Q4 2027
Go Live actions

- **PSD3 Go-Live - late 2027 into** 2028 (estimated, following 2026 adoption and transition).
- **EU AI Act Compliance - December 2027.**

8.5 Resource Requirements

UK Card Issuers

Small issuers (< 100k cardholders):

Smaller issuers can generally integrate Consumer Duty and AI governance changes into existing credit risk, compliance, and fraud-operations teams, with focused work on model governance, explainability, and customer communications.

Most of the effort lies in reviewing current credit decisioning and fraud systems, identifying where AI is used, and putting proportionate oversight and documentation around those models.

Large issuers (> 1M cardholders):

Large issuers with complex portfolios and higher fraud volumes will tend to require more structured programmes, covering model inventories, bias testing, explainability frameworks, and end-to-end customer journeys.

Dedicated resource from risk, data science, technology, legal, and compliance is likely, alongside enhanced MI and governance to satisfy both Consumer Duty and forthcoming FCA AI expectations.

EU Card Issuers

Small issuers:

Smaller EU issuers will need to plan for a combination of PSD3 changes (outcomes-based SCA, spoofing liability, spending limits) and EU AI Act requirements for high-risk AI used in credit and fraud.

This can often be handled by extending existing PSD2 and risk teams, with targeted projects to adjust SCA flows, add spending-limit controls, and introduce basic AI governance around credit and fraud models.

Large issuers:

Large EU issuers are likely to approach PSD3 and the EU AI Act as significant, multi-year programmes, given the scale of their customer base, product complexity, and model estates.

Expect sustained engagement from senior management, central programme teams, and multiple functions (risk, technology, operations, legal, compliance) to redesign SCA approaches, roll out new consumer protections, and embed AI governance across card decisioning and fraud detection.

Note: For banking groups, card-issuer resource planning should be folded into the broader PSD3/AMLR/AI programmes described in Chapters 7 and 9, not run as a separate transformation track.

8.6 What card issuers do NOT need to worry about

Safeguarding Obligations

Bank card issuers do not apply CASS 15 to cardholder funds: those balances sit under the bank prudential and capital framework, and card flows are governed by scheme rules rather than the PI/EMI safeguarding regime.

Non-bank issuers that are EMIs remain subject to CASS 15 for the underlying e-money they issue (see Chapters 1-2). This chapter does not repeat those EMI safeguarding rules.

APP Fraud Reimbursement

APP fraud liability applies to banks/PSPs in Faster Payments/CHAPS, not card issuers (card fraud governed by scheme chargeback framework).

BNPL Regulation

Unless separately offering BNPL products (separate regulatory framework, see Chapter 5).

8.7 Risk Factors & Mitigation

Regulatory Risks

RISK	MITIGATION
FCA enforcement on AI bias in credit decisioning	Regular bias testing, document testing results, maintain senior manager oversight.
PSD3 SCA requirements materially change (post-adoption)	Build flexibility into SCA systems, monitor EBA standards, participate in consultations

Operational Risks

RISK	MITIGATION
Fraud AI false positives create reputational damage (de-banking)	Continuous monitoring of false positive rates, appeals process, customer communication.

For bank issuers, these card-specific risks should be read alongside the wider fraud, CoP/APP reimbursement, AML and operational-resilience risks in Chapter 7 (see 7.6 for the bank-level risk view).

For EMI issuers and other non-bank issuers, they should sit within the same group-wide AI, fraud, safeguarding and operational-resilience risk frameworks described in Chapters 2 and 9 (see 2.6 for safeguarding-specific risks and Chapter 9 for cross-cutting AI, resilience and portfolio-level risks), rather than in a standalone "cards only" risk silo.

8.8 Key Takeaways

If you only remember four things from this chapter as a card issuer, make them these:

- **You live under card-scheme chargeback rules rather than APP reimbursement**, but PSD3 will still raise your fraud and spoofing-liability bar in the EU, and Consumer Duty will judge how fair your fraud and credit decisions are in the UK (see 7.2 for bank APP/CoP duties and 7.3.2 for EU spoofing).
- **Outcomes-based SCA under PSD3 is an opportunity**, not just a burden: issuers that invest in smarter fraud controls can reduce friction without falling foul of regulators, while those that simply bolt on more 3DS challenges will pay twice in fraud and lost spend (see 8.3.1 and 8.3.2 for the PSD3 card-issuer angle, and 7.3.2-7.3.3 for the bank/PSD3 fraud stack).
- **AI governance is not a "nice to have AI strategy deck"**; it is about being able to explain, evidence and, where necessary, override the models that approve, decline, limit and block your cardholders - in ways that satisfy Consumer Duty in the UK and the AI Act in the EU (see 8.2.1-8.2.2 for issuer examples, 7.1 and 7.6 for bank-level AI risks, and Chapter 9 for the cross-cutting AI themes).
- The safest way to implement all of this is to **treat card issuing as one product line inside a group-wide change portfolio for PSD3, AMLR, AI and resilience** (Chapters 7 and 9), not as a standalone compliance project bolted on at the end.

Chapter 9: Regulatory Divergence & Critical Integration Points

This chapter pulls together the cross-cutting patterns and UK/EU divergences that sit behind the stakeholder chapters.

9.1 UK vs EU Divergence at a Glance

The table below sets out the main fault-lines in one place before we look at how they interact in practice.

Dimension	UK Approach	EU Approach	What it means for you
Safeguarding deadline	CASS 15 from 7 May 2026 for UK-authorised PIs/EMIs holding relevant funds or e-money.	EMD2/PSD2 today for EMIs; PSD3/PSR from around Q4 2027 into 2028 for EU PSPs after 2026 adoption and transition.	UK PIs/EMIs move first; EU PIs/EMIs have a longer runway but a heavier end-state. See Chapters 1-2 for detailed safeguarding requirements and timelines.
Crypto authorisation	FSMA 2023 gateway 30 Sep 2026-28 Feb 2027; UK regime live 25 Oct 2027.	MiCAR already phasing in 2024-2026.	EU crypto firms are already in-regime; UK-facing firms have a tight 2026-2027 gateway window.
BNPL regulation	15 Jul 2026; merchant-financed BNPL exempt from authorisation.	20 Nov 2026; no general merchant exemption.	Third-party BNPL providers face dual regimes; UK merchants retain a relative cost advantage vs EU merchants offering BNPL.
Card issuer SCA	Principles-based SCA under FCA guidance (no PSD3 adoption).	PSD3 outcomes-based SCA from around Q4 2027.	Different models rather than a clear "winner"; EU issuers get more flexibility but more scrutiny on outcomes.
PISP/AISP access rights	PSD2-based UK regime; banks retain more practical control over API quality.	PSD3 strengthens PISP/AISP access, prohibits obstacles and opens up mobile-OS NFC on FRAND-style terms.	EU PISPs/AISPs gain stronger structural leverage over banks post-PSD3; UK PISPs remain in today's API landscape.
AI governance	FCA AI-governance guidance expected around Dec 2026, layered onto Consumer Duty.	EU AI Act from Dec 2027 for high-risk AI in financial services.	Both tighten AI expectations, but via different frameworks and timelines; cross-border groups need one AI governance approach that satisfies two regimes.

9.2 Integration & Interaction: How Stakeholders Intersect

Three interaction patterns cut across the stakeholder chapters in ways that materially change firms' risk and delivery loads.

9.2.1 Payment Institutions + Acquirers (Fund Holding Risk)

When a PI also acquires and holds merchant settlement funds in suspense, rolling-reserve or split-pay structures, CASS 15 safeguarding applies immediately in the UK from May 2026, and PSD3 safeguarding will follow for EU operations. If you are genuinely T+0/T+1 with no end-of-day balances, safeguarding does not bite.

In other words, it is the fund-flow and holding period, not the "acquirer" label, that determines whether you are in a full safeguarding regime or not; mis-classifying that model is a regulatory breach, not a harmless accounting choice.

9.2.2 PISPs + Banks (API Dependency)

Today, EU and UK PISPs still live with uneven bank API quality and residual practical obstacles, even though PSD2 and the RTS on SCA/CSC already prohibit many forms of throttling, extra consent steps and multiple SCAs that disadvantage third parties. In practice, some ASPSPs still design or operate APIs in ways that leave PISP journeys rougher or less reliable than their own channels, so PISPs depend on supervisory pressure and industry governance to keep those obstacles in check.

From around Q4 2027, PSD3 is expected to sharpen that position in the EU by explicitly defining and banning a wider range of "obstacles" and by tying API performance and NFC access to detailed technical standards, turning open-banking access more clearly into regulated infrastructure. UK PISPs, by contrast, remain in the current PSD2-based regime with FCA/PSR oversight but without a PSD3-style refresh, so EU PISPs gain relatively more structural leverage over banks than their UK counterparts.

9.2.3 Stablecoin Issuers + PSD3 (Dual Compliance Risk)

For EU stablecoin issuers, the key integration question is whether a token "walks and talks" like e-money under PSD3:

- If it does, you face potential dual compliance: MiCAR as a crypto-asset regime and PSD3 as an e-money and payment-services regime, including safeguarding and governance expectations.
- If it does not (for example an asset-referenced token), MiCAR alone applies.

The licensing and safeguarding detail sits in Chapters 2 and 4; the integration question here is whether you are designing for one regime or two.

Stablecoin issuers should also monitor any UK "equivalence" or substitutive-compliance decisions for major overseas regimes such as MiCAR and PSD3, as these could allow some home-state controls to count towards UK expectations and reduce the need for two entirely separate frameworks.

9.3 How to organise the work

9.3.1 Recommended governance for medium/large firms:

Regulatory Change Steering Committee: Prioritise initiatives, allocate budget, escalate blockers Chair: Chief Operating Officer or Chief Risk Officer

- Members: Heads of Compliance, Legal, Technology, Operations, Finance
- Frequency: Monthly

Workstream Leads

- Safeguarding Lead (if applicable)
- PSD3 Lead
- Crypto Authorisation Lead (if applicable)
- AI Governance Lead
- Operational Resilience Lead

Cross-Functional Squads

- Each workstream has squad: Compliance, Legal, Technology, Operations, Finance representatives
- Agile delivery methodology (sprints, standups, retrospectives)

9.3.2 Recommended governance for small firms:

- Single regulatory change lead (often the Head of Compliance or COO) with responsibility across all regimes, rather than separate workstream owners for each regulation.
- Small cross-functional project team drawn from operations, finance, and technology to support major deadlines, meeting weekly or fortnightly rather than running full agile squads.
- Targeted use of external advisers (legal, audit, specialist consultants) at key design and review stages, instead of building a large permanent change function.
- A simple, consolidated regulatory roadmap for the board and senior management, showing all relevant regimes and deadlines in one place, with clear RAG status and named owners.

Conclusion: The 2026-2027 Regulatory Reckoning

The Strategic Imperative

The UK and EU payments ecosystem faces simultaneous regulatory convergence and divergence. By 2027-2028, three major regimes go live: CASS 15 UK on 7 May 2026, PSD3/PSR in the EU after an estimated 18-21 month transition from 2026 adoption, and the UK crypto regime on 25 October 2027. Firms that move now gain first-mover advantages; laggards face forced compliance or market exit.

The Payments Forward Plan confirms that the 2026-2028 period will be managed against a single, integrated payments roadmap; this handbook offers the firm-level implementation view that sits alongside that public plan.

Integration & Interaction: How the Pieces Combine

Chapter 9 brought together the cross-cutting themes: how safeguarding, BNPL, crypto, open banking, cards, AI and operational resilience interact across stakeholder types, and where the UK and EU are converging or diverging. Firms that play more than one role should use the Stakeholder Impact Matrix and Chapter 9 to identify each role they perform, read the corresponding stakeholder chapters, and overlay the timelines and action lists into a single internal plan.

Three Non-Negotiable Actions (2026)

You can treat the rest of this roadmap as optional reading; these three actions are not.

1. **Business Model Classification (all stakeholders)**
   Legal scoping is non-discretionary. Fund holding, account structure and geographic scope each change regulatory burden by a factor of 5-10, and misclassification discovered after a deadline means enforcement action, remediation costs and, in extremis, forced business model change.
2. **UK Gateway Windows Close (crypto, BNPL)**
   - **Crypto: Gateway September 2026-February 2027**, with transitional protections only if you are inside that window.
   - **BNPL: 15 July 2026** is the line between authorised operation and exit from the UK market for third-party providers.
   - These dates do not move; firms applying early gain regulatory certainty and continuity, while late or non-applicants face forced closure or prolonged supervisory scrutiny.
3. **PSD3 Preparation Starts Now (EU operations)**
   Final text is expected in Q2 2026, adoption in late 2026, with implementation around Q4 2027 plus a 21-month transition. Early preparation (e.g. gap analysis, monitoring of technical standards, and engagement with supervisors and industry bodies) will separate firms that arrive at Q4 2027 ready to operate from those scrambling through last-minute remediation.

The Bottom Line

2026 is the year of regulatory clarity but also of deadline urgency. Firms that classify their business models correctly, use this roadmap to identify which regimes truly apply to them, apply during the critical gateway windows, and begin PSD3 preparation in Q1-Q2 2026 will be compliant and competitive by 2028. Firms that wait will face enforcement, forced restructuring or market exit.

The regulatory reckoning is now.

GET IN TOUCH



I hope you've enjoyed this handbook and found it of value, as producing it certainly clarified things in my own mind. If you have time, I'd love to hear your feedback!

Interested in learning more? I'd love to help you decode the payments world! My keynotes, training, and books make payments and fintech fun and accessible. Whether you need consulting, expert advice or training, I'll support your journey with 25+ years of experience in financial services. Let me transform your payment knowledge with a personal touch and a bit of humour!

My e-learning platform:
https://neirajones.thinkific.com/

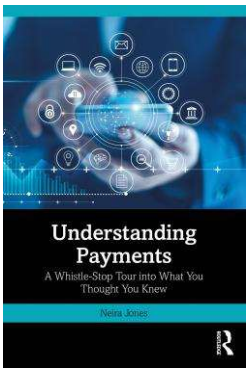
Book me for your event

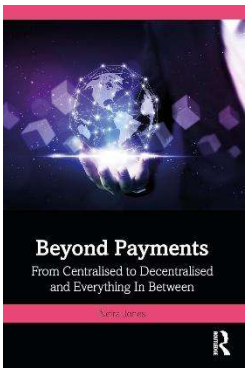
I regularly address global audiences, in person or virtually, with thought-provoking insights on payments, fintech, and related topics. From intimate boardrooms to bustling conference halls, I transform complex industry concepts into lively, accessible discussions.
Need a keynote that educates whilst entertaining? I deliver presentations that resonate long after the applause fades!

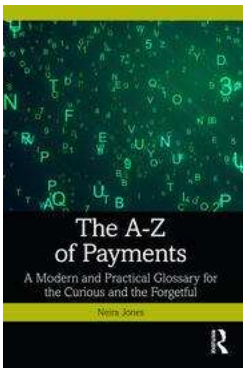
My books

Need help?

With over 25 years in financial services and technology, I'm passionate about change through innovation and partnerships, constantly demystifying the hype around industry trends. I advise organisations of all sizes on payments, fintech, regtech, cybersecurity, and regulatory matters. As a strategic board advisor and non-executive director, I take immense pleasure in collaborating with innovative companies, catalysing their growth through pragmatic guidance and industry savvy.







REFERENCES

[1] https://www.gov.uk/government/publications/payments-forward-plan

[2] https://www.fca.org.uk/publications/policy-statements/ps25-12-changes-safeguarding-regime-payments-and-e-money-firms

[3] https://www.fca.org.uk/firms/regulating-buy-now-pay-later

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A367%3AFIN

[5] https://eur-lex.europa.eu/EN/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes-from-2027.html

[6] https://www.fca.org.uk/firms/new-regime-cryptoasset-regulation

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114

[8] https://www.fca.org.uk/firms/new-regime-cryptoasset-regulation/how-gateway-will-operate

[9] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[10] https://www.psr.org.uk/publications/legal-directions-and-decisions/specific-direction-20-fps-app-scam-reimbursement-requirement/

[11] https://www.psr.org.uk/publications/legal-directions-and-decisions/specific-direction-21-chaps-app-scam-reimbursement-requirement/

[12] https://www.ecb.europa.eu/paym/retail/instant_payments/html/instant_payments_regulation.en.html

[13] https://www.ecb.europa.eu/paym/target/target-professional-use-documents-links/tips/shared/pdf/tipsmeetdoc/ecb.tipsmeetdoc240419_TIPS-CG_Verification_of_Payee_Service.en.pdf

[14] https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector]

[15] https://eur-lex.europa.eu/eli/dir/2023/2225/oj/eng

[16] https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/

[17] https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience

[18] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf

[19] https://standards.openbanking.org.uk/operational-guidelines/latest/