Plenitude

CBUAE Article 149 Fraud Readiness Playbook

January 2026

CBUAE Article 149: At a Glance

Plenitude

1 Who Does Article 149 Apply To?

- All Licensed Financial Institutions (LFIs) operating under CBUAE supervision.
- Applies across digital and traditional banking channels, including remote onboarding, authentication, transaction processing, and customer communication.
- Relevant to fraud-risk, operations, technology, cybersecurity, compliance, legal, and customer-facing teams.

2 What Firms Need To Do To Be Ready?

- **Immediate gap assessment** and prioritisation of fraud-prevention enhancements based on Article 149's mandatory obligations.
- **Implement robust fraud-prevention and detection controls.**
- **Align systems and processes** with forthcoming CBUAE minimum security standards.
- Strengthen fraud and breach notification processes, including escalation and customer communication.
- Establish reporting and data-submission capability to meet CBUAE fraud-information requirements.
- Put in place clear information-sharing and cooperation procedures to support supervisory requests.
- **Review customer-facing materials** to ensure clear, transparent, and accessible disclosures on fees, terms, and risks.

3 Potential Consequences of Non-Compliance

- Supervisory findings and mandated remediation.
- Financial Penalties / Fines up to AED 1 billion.
- Enforcement actions, including administrative penalties, directives, and conditions on the licence.
- Increased supervisory scrutiny, including enhanced reporting or on-site reviews.
- Customer harm and reputational impact due to delayed breach notifications or ineffective fraud controls.
- Operational and financial losses from unmitigated fraud risks.

4 Deadlines for Adoption

- One-year transition period, giving all persons subject to the Law until 16 September 2026 to reconcile their positions.
- Early adoption is encouraged to demonstrate proactive regulatory compliance, reduce supervisory risk, and ensure firms are fully prepared ahead of CBUAE reviews and enforcement of Article 149.

Practical Steps for Compliance

High-level Actions & Next Steps

To comply with CBUAE Article 149, firms must follow a structured, phased approach that strengthens fraud-risk governance, enhances operational resilience, and ensures readiness ahead of the transition deadline.

The below framework outlines the key steps organisations should take, from immediate actions to longer-term enhancements, helping LFIs build sustainable fraud-prevention capabilities aligned to regulatory expectations.

Action Area	Foundations for Compliance (Immediate Action)	Building Capability (3-6 Months)	Embedding (6+ Months)	Responsible Stakeholder
Governance & Accountability	• Assign senior sponsor and define accountability for Article 149 compliance. • Brief Board / ExCo on new obligations and transition timelines.	• Embed fraud-prevention responsibilities into governance committees. • Establish cross-functional working group (fraud, risk, IT, compliance).	• Formalise governance with annual reporting and board-level oversight. • Update governance to incorporate any CBUAE-issued standards.	• 1st LoD - Heads of Business Units • 2nd LoD - Chief Compliance Officer (CCO), Risk Director • 3rd LoD - Head of Internal Audit
Fraud Risk Assessment	• Conduct/ update Fraud Risk Assessment • Ensure that all products and services are reflected and documented.	• Develop organisation-specific fraud typologies aligned to Article 149. • Integrate findings into enterprise risk assessment.	• Ensure periodic review of risk assessments. • Update risk taxonomy for emerging fraud patterns.	• 1st LoD - Fraud Prevention Officers, Business Unit Risk Leads • 2nd LoD - Compliance, Financial Crime Teams • 3rd LoD - Internal Audit Function
Fraud Prevention & Detection Controls	• Review existing controls against Article 149 requirements. • Define enhancements for authentication, monitoring, and escalation.	• Implement strengthened controls (e.g., enhanced transaction/ payment controls, real-time monitoring, behavioural analytics). • Test updated controls and refine rules.	• Embed controls into enterprise frameworks (risk, operations, technology). • Prepare to meet minimum-security standards once issued under Article 149.	• 1st LoD - Fraud Prevention Teams, Risk Teams and Financial Controllers • 2nd LoD - MLRO's, Compliance & Legal Counsel
Customer Communication & Incident Response	• Review breach/fraud communication protocols. • Define triggers for prompt customer notification and corrective actions.	• Train frontline and incident teams on updated protocols. • Introduce customer-ready templates for transparent communication.	• Conduct simulations and refine notification playbooks. • Embed communication protocols into broader crisis/incident management.	• 1st LoD - HR, Line Managers, Business Unit Heads • 2nd LoD - Compliance Training Officers • 3rd LoD - Internal Audit for assurance
Regulatory Reporting & Supervisory Engagement	• Map data required under Article 149 (transaction records, patterns, mitigation measures). • Ensure readiness to respond to CBUAE information requests.	• Implement reporting mechanisms and quality controls for fraud-related data. • Document response processes for CBUAE inspections and directives.	• Maintain ongoing reporting cadence and respond to new CBUAE requirements. • Build audit-ready evidence of compliance.	• 1st LoD - Procurement Managers, Vendor Risk Leads • 2nd LoD - Third-Party Risk Teams, Compliance Officers
Customer Transparency & Disclosures	• Review clarity and accessibility of fee, terms, and risk disclosures. • Identify areas requiring simplification or improved visibility.	• Redesign customer-facing materials to meet transparency expectations under Article 149. • Test new materials with customer-facing teams.	• Periodically review disclosure effectiveness. • Update disclosures in line with new products, channels, or CBUAE rules.	• 1st LoD - Fraud & Financial Crime Teams • 2nd LoD - Compliance, Risk • 3rd LoD - Internal Audit

Practical Considerations & Implementation Challenges

Plenitude

Experience from implementing other financial-crime regulatory requirements shows that successful implementation depends not only on technical controls, but on addressing broader organisational challenges. This slide summarises the key considerations and potential obstacles LFIs must navigate to ensure effective, timely, and sustainable compliance with Article 149.

Action Area	Challenges	Considerations
Governance & Accountability	• Establishing clear ownership for Article 149 compliance across senior management. • Ensuring consistent oversight during the transition period through September 2026 (and any extensions). • Embedding fraud prevention within existing governance structures without creating duplication.	• Strong governance and documented rationale for decisions strengthen regulatory defensibility. • GCC regulators have issued findings for weak fraud-governance, reinforcing the need for strong oversight similar to Article 149.
Fraud Risk Assessment	• Developing tailored fraud risk assessments covering unauthorised transactions, social engineering, and identity theft. • Integrating emerging typologies and data sources into existing risk frameworks. • Avoiding generic, one-size-fits-all assessments.	• Robust, documented fraud risk assessments provide the evidential basis for demonstrating a clear understanding of product-specific fraud risks and the effectiveness of associated controls. • GCC regulators now require structured, typology-based fraud-risk assessments, mirroring Article 149's focus on tailored, documented risk analysis.
Fraud Prevention & Detection Controls	• Uplifting authentication, transaction monitoring, and detection controls in line with evolving CBUAE minimum standards, while managing legacy technology constraints. • Designing automated and real-time controls that balance fraud prevention effectiveness with accuracy, customer experience, and operational sustainability.	• Control enhancements should be risk-led and prioritised against the institution's fraud risk assessment, reflecting GCC regulatory expectations for stronger authentication and real-time fraud monitoring in response to rising social-engineering losses. • Automation and real-time monitoring require defined governance, tuning, and review mechanisms to manage false positives and customer impact.
Customer Communication & Incident Response	• Achieving genuinely prompt and transparent customer notifications following breaches or suspected fraud. • Coordinating legal, communications, operations, and customer-facing teams. • Maintaining readiness for real-time response.	• Well-defined, tested response playbooks reduce customer harm and reputational risk. • GCC regulators mandate detailed fraud reporting and have acted on late or inaccurate submissions.
Regulatory Reporting & Supervisory Engagement	• Collecting and validating fraud-related data to meet Article 149 reporting expectations across multiple systems • Responding effectively to CBUAE information requests and supervisory directives. • Maintaining evidence to demonstrate ongoing compliance over time.	• Strong data integrity, traceability, and ownership underpin accurate and timely regulatory reporting. • Proactive and transparent regulatory engagement reduces the risk of escalated supervisory scrutiny. • Repeatable reporting and evidence processes support sustained compliance, not just point-in-time readiness.
Customer Transparency & Disclosures	• Delivering clear, accessible, and customer-friendly fee, term, and risk disclosures consistently across products and channels, including digital journeys. • Remediating and maintaining legacy disclosure documents and digital content that were not designed for enhanced transparency expectations. • Sustaining alignment of disclosures as products, channels, and regulatory requirements evolve over time.	• Plain-language, customer-tested disclosures reduce complaints, support informed decision-making, and mitigate regulatory risk. • Disclosures should be subject to periodic review and formal change controls to ensure continued alignment with Article 149 as products and channels evolve. • Clear ownership for disclosure content across legal, compliance, product, and digital teams is critical to maintaining consistency and supervisory defensibility.

Final Thoughts: Staying Ahead of Compliance

With the one-year transition period ending on 16 September 2026 and certain related CBUAE security and fraud-control expectations being phased earlier, LFIs must act now to ensure full alignment with Article 149's strengthened fraud-prevention expectations. Early preparation will not only mitigate regulatory and legal exposure but also reinforce organisational resilience, customer protection, and trust in the financial system.

Article 149 elevates fraud prevention to a strategic priority. Firms should embed its requirements, risk assessments, enhanced controls, customer notification, information sharing, and transparent disclosures. within existing financial-crime frameworks rather than treating them as standalone activities. Organisations with strong governance, clear accountability, robust detection capabilities, and accurate reporting will be better positioned to meet evolving supervisory expectations.

Given the dynamic nature of fraud threats, compliance under Article 149 is not a one-time exercise. LFIs must commit to continuous improvement, adapting fraud-prevention measures as new typologies, technologies, and regulatory standards emerge. This requires coordinated efforts across fraud, compliance, cybersecurity, risk, legal, operations, and customer-facing teams.

Ultimately, Article 149 should be viewed not merely as a regulatory requirement but as an opportunity to strengthen operational resilience, improve customer outcomes, and enhance competitive advantage. Firms that build integrated, well-governed fraud-prevention frameworks will be better able to navigate scrutiny, reduce financial and reputational risk, and maintain stakeholder confidence.

How Plenitude Can Support Firms

Plenitude provides end-to-end support to help LFIs assess their readiness, implement the right enhancements, and build sustainable fraud-prevention capabilities aligned to CBUAE Article 149. Our practitioner-led model combines deep fraud, risk, and compliance expertise with hands-on transformation and systems optimisation.

As an FCA-appointed Skilled Person for Financial Crime, we bring insight from one of the world's most mature regulatory environments, complemented by extensive experience supporting firms across Europe, the Middle East, and Asia.
This combination gives us a clear, practical view of what "good" looks like in fraud governance, controls, reporting, and customer protection, positioning us strongly to support firms responding to heightened expectations under Article 149.

Our practitioner-led model combines deep fraud, risk, and compliance expertise with hands-on transformation and systems optimisation.

Together, our service lines provide a coherent journey:
assess → transform → optimise, enabling firms to strengthen defences, meet regulatory expectations, and continuously adapt to evolving fraud threats.

1

Fraud Independent Assessment

Objective: Identify control gaps and assess Article 149 readiness.

What We Provide:
- Independent, regulatory-grade review of fraud controls, monitoring, customer notification, and reporting.
- Typology mapping (scams, ATO, mules, ID theft) to detect vulnerabilities.
- Governance and MI assessment, with a prioritised remediation roadmap.

Outcome: A clear, defensible picture of readiness and targeted improvements, informed by standards expected in jurisdictions with high regulatory maturity.

2

Fraud Transformation

Objective: Build sustainable, Article 149-aligned fraud-management capabilities.

What We Provide:
- Enhanced fraud strategy, operating model, governance, and reporting, consistent with regulatory grade expectations.
- Upgraded incident response and customer-notification processes.
- Delivery of remediation actions and wider transformation support.

Outcome: Stronger resilience, improved audit readiness, and better customer protection, drawing on the same methodologies we apply during Skilled Person reviews.

3

Fraud Systems Optimisation

Objective: Ensure high-performing, compliant fraud-detection systems.

What We Provide:
- Expert tuning of rules, models, thresholds, and monitoring, aligned to leading industry and supervisory practices.
- Strengthened system governance, documentation, and MI.
- Ongoing SME support for new typologies and regulatory changes.

Outcome: Optimised performance, fewer false positives, and enhanced regulatory confidence, supported by expertise gained assessing system effectiveness in mature regulatory markets.

About Plenitude

Plenitude provides market-leading Fraud and Financial Crime Compliance (FCC) advisory, transformation, technology, data analytics, and managed services. We are committed to building a secure financial system, safeguarding society, and empowering our clients to meet their regulatory obligations.

Appointed to the FCA's Skilled Person Panel for Financial Crime, we help clients stay ahead of emerging risks and evolving regulations by optimising systems and controls and leveraging the latest AI-enabled technology and data analytics. Our best-in-class team, drawn from multiple disciplines across financial crime, risk, technology, operations, and regulatory compliance, delivers scalable, high-quality solutions that inspire confidence and drive sustainable outcomes.

We work with a wide range of retail, commercial and investment banks, insurers, asset managers, payment service firms, electronic money institutions, FinTechs, and crypto firms globally, from startups to the largest international financial institutions. Our track record includes advisory and transformation engagements on some of the most complex regulatory programmes in the market.

Our depth of expertise, commitment to integrity, and consistent delivery excellence have been recognised by many clients. Discover how our services, innovation, and pragmatic approach can support your organisation's fraud-prevention and financial crime objectives.

Our Fraud Advisory and Transformation services leverage proprietary toolkits and methodologies refined through extensive engagements across global financial institutions. These capabilities align with CBUAE Article 149, supporting firms to strengthen fraud-risk governance, enhance controls, implement clearer customer-notification processes, and meet regulatory expectations during the transition period to 16 September 2026.

We help LFIs:

- **Build governance**, accountability, and oversight structures aligned to Article 149.
- **Conduct independent assessments** of fraud-detection effectiveness, typology coverage, and risk-exposure.
- **Enhance customer-communication** frameworks to meet requirements for prompt, transparent notifications.
- **Strengthen reporting processes**, MI, audit trails, and evidence packs required under Article 149.
- **Optimise fraud-prevention systems**, controls, and operational models to ensure sustainable compliance.

Our comprehensive suite of services supports firms across all internal and external fraud risks, helping them build resilient, Article 149-aligned frameworks that can adapt to evolving regulatory expectations and emerging fraud threats.

Chris Bone,
Managing Director
Fraud Practice Lead

Tom Nickelson,
Senior Manager

Dovile Morkuaite,
Senior Manager

Matt Hawes,
Manager

Heather Thomson,
Senior Consultant