REGULATORY POLICY SEMINAR PAPER

SEMINAR PAPER — SUBMITTED TO THE FINANCIAL CONDUCT AUTHORITY AND INDUSTRY STAKEHOLDERS

THE UNFINISHED LAW:

WHY CASS 15 CANNOT WORK WITHOUT A MANDATORY CERTIFIED CASS SAFEGUARDING OFFICER

A Case for Regulatory Completion, Professional Certification, and the Creation of a New Specialist Profession in the United Kingdom Fintech Compliance Sector

AUTHOR

Olushola Oke-Daniel

Barrister and Solicitor of the Supreme Court of Nigeria

Founder & Director, AFC Fintech Ltd ·

Inventor, Sovereign Auditor Machine — Automated CASS 15 Compliance Engine with Human-in-the-Loop Governance

CONTRIBUTOR & REGULATORY REVIEWER

Dr Kolawole Oyekan

Chief Regulatory Director, AFC Fintech Ltd ·

Regulatory Anchor: FCA PS25/12 · CASS 15 · Effective 7 May 2026

Submitted: March 2026 · Version 1.0

Contact: olushola@fintechafc.co.uk · 07473 735 005

Author's Note

This paper is written from a dual perspective that is unusual in regulatory policy discourse and which the author believes gives it a distinctive and, in the present circumstances, essential analytical value.

The author, Olushola Oke-Daniel, is a Barrister and Solicitor of the Supreme Court of Nigeria with formal legal training and professional experience across multiple jurisdictions. He writes, therefore, as a lawyer — trained to read statutes carefully, to identify gaps and ambiguities in regulatory frameworks, and to reason from legal principle to practical consequence.

He also writes as a technologist and inventor. The author is the inventor of the Sovereign Auditor Machine — an automated compliance processing system specifically designed to enable Electronic Money Institutions and Payment Institutions to meet the daily reconciliation obligation imposed by the Financial Conduct Authority's CASS 15 framework. The Sovereign Auditor Machine operates on a human-in-the-loop governance model: it processes, analyses, and surfaces compliance findings, but every compliance determination it produces must be reviewed and authorised by a qualified human professional before delivery. The system was designed this way deliberately — to satisfy the requirements of GDPR Article 22 and to create a compliance output that carries genuine regulatory legitimacy, not merely the appearance of it.

This dual perspective — law and technology — places the author in a position to identify a gap in the regulatory framework that is invisible from either perspective alone. From the legal perspective, the gap is a missing mandatory appointment provision. From the technological perspective, the gap is a missing qualified human to operate the tools that compliance technology makes available. These two missing pieces are the same missing piece. This paper names it and argues for it to be filled.

Dr Kolawole Oyekan, Chief Regulatory Director of AFC Fintech Ltd, has contributed to the regulatory analysis in this paper and has reviewed its conclusions. The author acknowledges his contribution with gratitude.

> *Compliance technology has created the instrument. The law has not yet created the professional who is formally qualified to operate it. This paper is the argument for why the law must do so — and urgently.*

CONTENTS

Abstract

This paper argues that the Financial Conduct Authority's Policy Statement PS25/12 and its accompanying CASS 15 framework, while a significant and necessary step forward in the protection of client money in the United Kingdom payments sector, is structurally incomplete. It creates a sophisticated, technically demanding, daily operational compliance obligation on over 900 regulated firms without simultaneously requiring those firms to employ a specially trained, dedicated, and certified professional to discharge it.

The paper draws a direct and sustained comparison with the data protection framework under the UK General Data Protection Regulation, which both creates the compliance obligation and mandates the appointment of a Data Protection Officer for qualifying organisations. It argues that the same legislative logic applies — with even greater force — to CASS 15, where the daily operational burden is heavier, the technical knowledge more specialised, and the regulatory exposure broader: encompassing FCA safeguarding law, UK data protection law, and cybersecurity governance simultaneously.

The paper further argues that the imposition of personal liability on Senior Manager Function holders under the Senior Managers and Certification Regime, without a corresponding mandatory training standard or certified professional appointment requirement, creates the structural conditions for regulatory injustice. Senior Managers are held to a standard of competence for which no formal qualification pathway exists. This is not accountability — it is the appearance of accountability imposed upon individuals who were never given the institutional means to comply.

Drawing on the author's own experience as a lawyer and as the inventor of the Sovereign Auditor Machine — a purpose-built automated compliance system for CASS 15 — the paper argues that the combination of certified human expertise and approved automated tooling is the only sustainable compliance model for the sector. It concludes by proposing a specific policy framework for a mandatory Certified CASS Safeguarding Officer appointment requirement, and identifies the substantial economic, professional, and social opportunities that such a framework would create.

> *The law has created the obligation. The law has attached personal liability to named individuals for its discharge. The law has not created the professional whose specific purpose is to discharge it. Until it does, enforcement against those individuals is structurally unjust. This paper is the case for completing the law.*

1. Introduction: A Law With a Missing Piece

1.1 The Problem, Stated Simply

Let us begin with a simple observation that, once made, cannot be unmade.

On 7 May 2026, the Financial Conduct Authority's Policy Statement PS25/12 takes full legal effect. From that date, every Electronic Money Institution and Payment Institution holding client money in the United Kingdom — over 900 of them — must perform a reconciliation of every penny of client money, every single business day. They must produce written evidence that the money is properly protected. They must detect any shortfall or commingling immediately. They must maintain a contemporaneous, timestamped audit trail. They must report breaches to the FCA within a defined and very short window.

This is not a light obligation. It is a daily, technically complex, legally consequential operation. And the individual named as responsible for it within each firm is personally liable under the Senior Managers and Certification Regime if it goes wrong.

Now here is the observation: nowhere in the CASS 15 framework, PS25/12, or any accompanying FCA guidance does the law specify that the person performing this daily operation must be formally trained, professionally certified, or hold any defined qualification. There is no mandatory appointment of a CASS specialist. There is no prescribed competence standard. There is no recognised professional title. There is, in the fullest legal sense of the phrase, no job description.

> *Imagine a surgeon being held personally liable every time a surgical procedure goes wrong — but the law never required that the person performing the surgery be a qualified surgeon, never created a surgical qualification, and never mandated that surgeons be appointed. You would not call that a regulatory framework. You would call it a trap.*

This paper argues that CASS 15, as currently framed, is precisely that trap. The obligation is real. The liability is real. The professional — the certified, trained, formally appointed specialist whose entire professional purpose is to discharge the obligation — does not yet exist in any formally mandated sense.

This paper is the argument for creating that professional. It draws on three sources of authority: legal analysis of the existing regulatory framework; direct comparison with the precedent set by the GDPR's Data Protection Officer mandate; and the practical insight of the inventor of the Sovereign Auditor Machine — purpose-built automated compliance technology — who understands, from that experience, precisely what knowledge and capability the daily compliance operation requires.

1.2 Why This Author Is Positioned to Make This Argument

The author brings an unusual combination of perspectives to this analysis. As a Barrister and Solicitor of the Supreme Court of Nigeria, the author is trained to read legislative frameworks precisely — to identify what a law says, what it implies, and what it silently assumes. The reading of CASS 15 offered in this paper is a lawyer's reading.

The author is also the inventor of the Sovereign Auditor Machine — an automated compliance processing system designed specifically to enable EMIs and PIs to discharge the CASS 15 daily reconciliation obligation. That system was engineered to solve one specific, technically demanding, legally consequential daily problem — and building it required the author to understand the CASS 15 compliance process from the inside.

That operational understanding is what gives this paper its particular analytical force. The author does not merely argue in the abstract that CASS 15 requires a trained professional. He argues it from the position of someone who has built compliance technology for this exact regulatory obligation — and who knows, from that experience, that no instrument, however sophisticated, can substitute for the professional judgement, regulatory knowledge, and personal accountability of a trained human being.

1.3 Structure of This Paper

The paper proceeds as follows. Section 2 explains, in plain language, what CASS 15 actually requires — because the gap in the framework is impossible to understand without first understanding the obligation the framework creates. Section 3 draws the comparison with the GDPR DPO framework and asks why the logic that produced the Data Protection Officer has not been applied here. Section 4 analyses the triple compliance burden — the simultaneous demands of FCA safeguarding law, UK GDPR, and cybersecurity governance — that any CASS practitioner must navigate daily. Section 5 addresses the injustice of Senior Manager liability without professional support. Section 6 presents the proposed policy solution, including the role of automated compliance technology within a human-in-the-loop compliance model. Section 7 identifies the economic and professional opportunities that a mandatory CASS profession would create. Section 8 addresses likely objections. Section 9 sets out specific recommendations. Section 10 concludes.

2. What CASS 15 Actually Demands — in Plain Language

2.1 The Obligation, Explained Without Jargon

CASS 15 requires that every EMI and PI holding client money must, on every single business day, do the following things:

- Check that every single client's money is held in a separate, ring-fenced account — one that belongs to that client and cannot be touched by the firm's creditors if the firm collapses.
- Compare what the firm's records say should be in that account against what is actually there. Every penny must be accounted for.
- Spot any shortfall — any gap between the records and reality — immediately, and report it.
- Spot any commingling — any mixing of client money with the firm's own money — immediately, and report it.
- Confirm that the evidence proving the ring-fencing is recent, complete, and in the right format.
- Write all of this down, with a timestamp, in a way that can be shown to the FCA at any moment, on demand.

> *Here is the equivalent in everyday terms: imagine being required, every single working day, to check that every locker in a changing room contains exactly what its owner said they put in it, that none of the lockers have been shared without permission, and that you can prove in writing — by close of business — that you checked every single one. Now multiply that changing room to hundreds of clients. That is CASS 15.*

2.2 Why This Is Different From Any Other Compliance Task

Most regulatory compliance in financial services operates in cycles. Anti-money laundering checks are triggered by specific transactions. Risk assessments are done quarterly. Reports are filed annually. An individual compliance officer can manage these obligations alongside other responsibilities because they do not all hit at once, every day, without exception.

CASS 15 is not cyclical. It is continuous. It is every business day. There is no day off. There is no batch processing. A client's money is either protected today, or it is not protected today. If the reconciliation does not happen today, the firm does not know whether a shortfall has arisen today. And if a shortfall has arisen, the firm is already in breach — from the moment the gap opened, not from the moment someone noticed it.

This is a critically important point that deserves emphasis: under CASS 15, ignorance is not a defence. The breach clock starts when the shortfall occurs, not when it is discovered. A firm that misses its daily reconciliation on Monday and discovers on Friday that a shortfall has existed since Monday has been in breach for four business days. The FCA will treat it that way.

THE DAILY CLOCK

Every business day without a completed, documented, timestamped reconciliation is a day on which the firm cannot demonstrate compliance. If the FCA requests evidence and the record for any given day is missing, the firm is treated as non-compliant for that day — regardless of what was actually done. The audit trail IS the compliance. You cannot separate them.

2.3 The Knowledge the Task Requires

To discharge the CASS 15 daily reconciliation competently — not superficially, not performatively, but in a way that would withstand FCA scrutiny — the person responsible must understand:

- The legal architecture of CASS 15: what it requires, what it prohibits, what evidence it demands, and how the FCA interprets those requirements in practice
- The mechanics of safeguarding account structures: the difference between individual client accounts and pooled accounts, and the specific evidence required for each
- How to identify a safeguarding shortfall and distinguish it from a legitimate balance fluctuation
- How to identify a commingling event and distinguish it from an authorised cross-client transaction
- The FCA's reporting threshold: the precise conditions under which a breach must be notified to the regulator, and how quickly
- UK GDPR obligations: because the daily process handles the personal financial data of potentially hundreds of clients, and every handling decision creates data protection exposure
- Cybersecurity protocols: because the data being handled is among the most sensitive that exists, and the systems being used to handle it must meet a defined security standard
- Professional ethics: because the practitioner is operating in a space where client interests, firm interests, and regulatory interests can diverge — and the right call is not always the comfortable one

This is not one knowledge domain. It is four: regulatory law, data protection, cybersecurity, and professional ethics. Each of these domains is a full professional discipline in its own right. A person who is expert in one is not automatically competent in the others. The CASS 15 daily reconciliation requires all four, simultaneously, every day.

Knowledge Domain	Why It Is Required in the CASS 15 Context	What Happens Without It
CASS 15 / FCA Regulation	Defines the specific obligations, evidence standards, and escalation requirements	Reconciliation done incorrectly or incompletely; breach undetected or unreported; FCA enforcement
UK GDPR / Data Protection	Every client record touched in the daily audit is personal data — lawful basis, minimisation, Article 22 compliance,	ICO investigation running alongside FCA investigation; concurrent fines from two regulators

	breach notification all apply	
Cybersecurity Governance	Client financial data is high-value; systems must be secured; credential management and encrypted data transfer are minimum standards	Data breach; system compromise; FCA operational resilience failure; ICO notification triggered
Professional Ethics	The practitioner may face pressure from clients or firm management not to report a breach; independence and integrity are non-negotiable professional duties	Suppression of findings; false audit trail; criminal liability; career destruction

3. The Precedent: What the GDPR Got Right

3.1 The Data Protection Officer — A Law That Completed Itself

In May 2018, the General Data Protection Regulation came into force, and with it one of the most consequential professional mandate provisions in modern regulatory history: Article 37, which required certain categories of organisation to appoint a Data Protection Officer.

The logic behind the DPO mandate was straightforward, and it is worth stating it precisely because it is the same logic that applies, with equal force, to CASS 15. The GDPR created a compliance obligation. That obligation was complex, technically demanding, and legally consequential — involving the processing of personal data on a scale and at a level of complexity that required specialist knowledge to get right. The GDPR's architects recognised that creating the obligation without simultaneously mandating the professional who would discharge it was incomplete legislation. They completed the law by creating the DPO.

> *The GDPR lawmakers asked: who is going to actually do this? They answered that question in the statute itself. Article 37 is the answer. It says: you must appoint a professional whose specific job is to ensure that your organisation complies with data protection law. The professional must be named. The professional must be qualified. The professional must be registered with the regulator. That is a complete legal framework.*

The consequences of that decision are now visible across the entire economy. There are thousands of practising Data Protection Officers in the United Kingdom. There are accredited university courses, professional certifications, and industry bodies dedicated to the profession. The International Association of Privacy Professionals has over 100,000 members worldwide. An entire ecosystem of training, certification, research, and practice was created because the law said: this obligation requires a professional, and that professional must exist.

3.2 The Direct Comparison

Now apply the same analytical lens to CASS 15. The comparison is direct and, on every material dimension, the case for a mandatory CASS professional is at least as strong as the case for the DPO — and in several respects stronger.

Dimension	UK GDPR — Data Protection Officer	CASS 15 — No Equivalent Yet
Is the obligation daily?	No — most GDPR obligations are event-triggered (breach, DSAR, new processing) or periodic (DPIA review, consent renewal)	YES — daily reconciliation every single business day, 260 days per year, without exception
Does it require specialist knowledge across	Yes — data protection law is complex, but the domain is primarily	YES — AND it spans three distinct regulatory regimes simultaneously:

multiple domains?	one framework	FCA law, UK GDPR, and cybersecurity
Does personal liability attach to a named individual?	Yes — DPO is accountable; ICO can pursue individuals; firms face fines up to £17.5m	YES — SMCR Senior Manager is personally liable; FCA can prohibit them from all regulated roles permanently
Has the law mandated a named, certified professional?	YES — Article 37, UK GDPR; DPO must be designated, registered with ICO, and sufficiently expert	NO — CASS 15 imposes the obligation and the liability but mandates NO equivalent professional appointment
Does a recognised professional qualification exist?	YES — CIPP/E, BCS DPO Practitioner, and many university-accredited programmes exist and are actively marketed	NO — no nationally accredited CASS Safeguarding Lead qualification currently exists in the UK
Has a certification register been established?	YES — ICO DPO register; firms must submit DPO contact details and can be contacted directly by the supervisory authority	NO — no CASS practitioner register exists; FCA cannot identify who performs the daily reconciliation at any given firm

THE CRITICAL ASYMMETRY

The GDPR imposes personal accountability AND mandates a certified professional to discharge the obligation, with a registration requirement so the regulator always knows who that professional is. CASS 15 imposes personal accountability WITHOUT any of those supporting structures. One of these approaches is complete legislation. The other is not.

3.3 The DPO Mandate Was Not Without Controversy — And It Still Worked

It is worth acknowledging that the DPO mandate was controversial when it was introduced. Industry groups argued it was burdensome. Small firms complained that it was disproportionate. Lawyers debated the boundary between DPO functions and legal advice. These debates were real, and they were not entirely without merit.

But the outcome is not in serious dispute. The DPO mandate improved data protection compliance. It created a professional discipline where none had existed. It gave the ICO a named contact at every qualifying organisation. It stimulated a training and certification market. And — crucially for the argument being made in this paper — it created thousands of jobs, many of them high-skill, well-paid positions in the compliance, legal, and technology sectors.

The same arguments that were made against the DPO mandate will be made against a mandatory CASS Safeguarding Officer requirement. This paper addresses those arguments in Section 8. The short answer is: the DPO objections were overridden by the value of the outcome. The CASS objections should be treated the same way.

4. The Triple Compliance Burden: One Person, Three Laws, Every Day

4.1 A Problem That Rarely Appears in the Headlines

When commentators discuss the compliance challenge created by CASS 15, the focus is typically on the FCA safeguarding obligation itself — the daily reconciliation, the audit trail, the reporting thresholds. This is understandable. CASS 15 is the headline requirement, and it is demanding enough in isolation.

What is less often discussed — and what the author, as both a lawyer and a system builder, has had occasion to examine in considerable depth — is that CASS 15 compliance does not happen in a legal vacuum. The person performing the daily reconciliation is, simultaneously, subject to obligations under two other distinct and fully operational legal frameworks: the UK General Data Protection Regulation and cybersecurity governance law. Each framework has its own rules. Each has its own regulator. Each has its own enforcement consequences. And compliance with one does not guarantee compliance with the others.

> *Imagine being required to cook a meal that simultaneously satisfies a Michelin-starred chef's standards (CASS 15), a nutritionist's dietary requirements (UK GDPR), and a food safety inspector's hygiene regulations (cybersecurity) — and being told that you will be fined separately by all three if you fail any one of them. That is not one job. That is three professional disciplines compressed into one daily task, performed by one person, with no time off.*

4.2 Layer One — FCA Safeguarding Law

The first and most visible layer is the CASS 15 obligation itself. The author has described this in detail in Section 2 and will not repeat it here. The key point for the triple-burden analysis is that CASS 15 compliance requires specific, non-trivial regulatory knowledge. A practitioner who does not understand the difference between a safeguarding shortfall and a timing difference, or who does not know the FCA's reporting threshold for a commingling event, or who has not understood the evidence renewal requirement for a pooled safeguarding account, is not a compliant practitioner — regardless of how diligently they show up to work every day.

The consequences of FCA non-compliance are: regulatory fines, licence restriction, licence revocation, and — for the named Senior Manager — personal financial penalties, public statements of misconduct, and permanent prohibition from holding any FCA-regulated Senior Manager Function.

4.3 Layer Two — UK GDPR and Data Protection Law

The second layer is the UK General Data Protection Regulation, enacted by the Data Protection Act 2018. Its relevance to the CASS 15 daily reconciliation is direct and unavoidable.

Every client record processed in the daily reconciliation is personal data. In most cases, it is sensitive personal data — financial information that reveals a great deal about a client's economic circumstances, business activities, and commercial relationships. Every time the practitioner opens that record, uploads it to a processing system, reviews a balance, or writes a finding note, they are processing personal data under the UK GDPR.

This creates, simultaneously with the CASS 15 obligation, the following GDPR obligations:

- Identifying and maintaining a lawful basis for processing each client's financial data in the CASS 15 context
- Applying data minimisation — using only the data necessary for the reconciliation and not retaining more than needed
- Complying with GDPR Article 22: because any automated compliance system produces structured analytical findings, those findings must be reviewed and authorised by a human professional before they become a compliance determination — the automated output alone is not sufficient
- Maintaining data retention schedules: CASS 15 records must be kept for a specified period but no longer, and deleting them prematurely or retaining them indefinitely both create GDPR exposure
- Notifying the ICO within 72 hours of a personal data breach — if a client's financial data is compromised during the reconciliation process, the practitioner must identify it and report it within a very short window

The ICO enforces these obligations independently of the FCA. A failure in the GDPR layer of a CASS 15 reconciliation can result in concurrent ICO and FCA enforcement — two separate investigations, two separate fine regimes, and two separate sets of reputational consequences. The maximum ICO fine is £17.5 million or 4% of global annual turnover — which, for a small fintech, is existential.

4.4 Layer Three — Cybersecurity Governance

The third layer is cybersecurity. It is the least visible of the three in regulatory discussions but it is the most operationally present. Every step of the CASS 15 daily reconciliation involves the use of technology.

Every step of the CASS 15 daily reconciliation involves the use of technology: accessing financial systems, uploading client data files, running processing software, generating output reports, transmitting determinations. Each of these steps creates a cybersecurity surface. And each of them, if handled without adequate cybersecurity discipline, creates the conditions for a data breach that triggers not just cybersecurity

enforcement but cascades into the GDPR layer (ICO notification) and potentially the FCA layer (operational resilience failure).

- The practitioner must operate from a secure, approved device with current endpoint security — not a home laptop shared with other users
- Authentication must use multi-factor verification; credentials must never be shared; session tokens must not be allowed to persist
- Compliance practitioners are specifically targeted by phishing attacks because they hold privileged access to personal financial data — awareness of this threat is not optional, it is a professional survival skill
- All data in transit must be encrypted; no client financial data may be sent over unverified channels
- Any cybersecurity incident that results in client data exposure triggers concurrent GDPR and potentially FCA notification obligations

> *Purpose-built CASS 15 compliance technology should be designed with a local-processing architecture precisely because cloud data transfer is an additional cybersecurity and GDPR risk that most compliance tools create unnecessarily. Client data should never leave the client's environment — a deliberate privacy-by-design and security-by-design principle. But even with the best-designed tool, the practitioner operating it must understand why those protections exist — and what to do when they are threatened.*

4.5 The Compounded Effect

Taken together, the triple compliance burden means that a single error in the daily CASS 15 reconciliation can create simultaneous enforcement exposure under three separate regulatory regimes. The practitioner who accidentally emails an unencrypted client balance sheet to the wrong address has, in one action: potentially breached CASS 15 (the client's data is not adequately secured), breached UK GDPR (personal financial data has been disclosed without authorisation), and triggered a cybersecurity incident that may constitute an operational resilience failure under the FCA's SYSC framework.

Compliance Layer	Regulator	Max Sanction	Triggered By
CASS 15 (FCA)	Financial Conduct Authority	Unlimited fine + licence revocation + personal SMF prohibition	Failure of daily reconciliation, inadequate audit trail, unreported breach
UK GDPR (ICO)	Information Commissioner's Office	£17.5m or 4% of global turnover	Unlawful data processing, breach notification failure, Article 22 violation
Cybersecurity (FCA/ICO/NCSC)	FCA (SYSC/DORA) + ICO + NCSC	Concurrent FCA and ICO enforcement	Inadequate system security, data breach, credential compromise, unencrypted transfer

No reasonable person would expect an individual to navigate this triple burden competently without dedicated, structured, formally assessed training that covers all three layers. And yet, under the current CASS 15 framework, this is precisely what is

expected. The law says: comply. It does not say: here is the professional who is trained to help you comply, and here is how you find and appoint them.

5. The Injustice: Personal Liability Without Professional Infrastructure

5.1 What the SMCR Was Designed to Achieve

The Senior Managers and Certification Regime is a well-intentioned and largely sound regulatory framework. It was introduced in the aftermath of the 2008 financial crisis, when a central lesson of that catastrophe was that responsibility within financial institutions had become so diffuse that no one could be held accountable for anything. The SMCR was the legislative response: named individuals, designated responsibilities, personal accountability.

The principle is defensible. When a major compliance failure occurs, the question 'who was responsible?' should have a clear and specific answer. The SMCR ensures that it does. The Senior Manager who holds the CASS responsibility is personally accountable. They cannot point to a committee, a team, or a policy document. They are the responsible person.

5.2 Where the Framework Becomes Unjust

Individual accountability is only fair — morally and legally — when the individual had access to the means to fulfil their responsibility. You cannot hold a person accountable for failing to do something that the regulatory framework provided them no practical means of doing.

This is the point at which the SMCR's application to CASS 15 becomes problematic. The framework places personal liability on the Senior Manager for the adequacy of the CASS 15 compliance function. But the framework does not:

- Specify what standard of training or qualification the person performing the daily reconciliation must hold
- Create or mandate a professional qualification that the Senior Manager could require their CASS practitioner to obtain
- Establish a register through which the Senior Manager could verify that their CASS practitioner meets a recognised professional standard
- Create a recognised professional class of CASS specialists whom the Senior Manager could confidently appoint

The Senior Manager is therefore in the following impossible position: they are personally liable for a function that requires specialist expertise; there is no professionally recognised route to acquiring that expertise; there is no one they can appoint with confidence that the appointee meets a defined professional standard; and — if something goes wrong — they will be asked to demonstrate that they took all reasonable steps, against a benchmark that the law has never defined.

> *This is equivalent to holding a building manager personally liable for the*

> *safety of the building's electrical installations, while simultaneously providing no electrician qualification, no licensed electrician register, no prescribed electrical safety standard, and then prosecuting the manager when the wiring fails. The liability is real. The means to discharge it safely were never provided. This is not accountability. This is a trap with legal authority behind it.*

5.3 The FCA's Enforcement Approach and What It Will Produce

The FCA has explicitly signalled that CASS 15 enforcement will be a supervisory priority from May 2026. This is appropriate. Protecting client money is a core regulatory objective, and the FCA is right to take it seriously.

But the enforcement approach that the current framework creates is foreseeable — and foreseeable injustice is avoidable injustice. In the absence of a mandatory professional standard, the FCA's enforcement investigators will be required to assess 'reasonable steps' against an undefined benchmark. In practice, this means that the investigation will be shaped by what the FCA's own staff believe a competent CASS practitioner should have done — a standard that has never been publicly specified, never been the subject of an accredited training programme, and never been validated through formal professional assessment.

THE FORESEEABLE OUTCOME

Senior Managers at small fintechs will face personal enforcement action for CASS 15 failures. Many of those failures will be attributable, at least in part, to the absence of trained, certified professionals to perform the daily reconciliation. The Senior Managers will not be able to demonstrate 'reasonable steps' because no reasonable step — in the form of a recognised qualification or a certified appointment — was ever made available to them. The FCA will enforce its rules against individuals who were structurally prevented from meeting the standard those rules implied.

5.4 A Historical Parallel — and a Lesson

This is not the first time that a regulatory framework has created this kind of structural gap. The financial crisis itself was partly the product of regulatory frameworks that imposed complex obligations without adequately defining the professional standards required to discharge them. The Approved Persons Regime — which the SMCR replaced — failed partly because it was never clear enough about what an 'approved person' was actually required to know and demonstrate.

The lesson of that history is that regulatory frameworks which create obligations without professional infrastructure do not produce compliance. They produce the appearance of compliance from firms that are trying, and unprosecuted non-compliance from firms that are not. They do not make clients safer. They make Senior Managers more vulnerable.

The FCA has the opportunity, right now, before the 7 May 2026 deadline produces the first wave of enforcement actions, to complete the CASS 15 framework. The mechanism is well-established. The precedent exists. This paper proposes how to use it.

6. The Solution: A Mandatory Certified CASS Safeguarding Officer

6.1 The Proposed Framework

The author proposes that the FCA, through a targeted and proportionate amendment to the CASS 15 regulatory framework, introduce a mandatory requirement for every regulated EMI and PI above a defined threshold to appoint a named, certified CASS Safeguarding Officer — a professional who holds a recognised qualification specifically covering CASS 15 regulation, UK GDPR obligations in the client money context, cybersecurity governance, and professional ethics.

This is not a novel or untested approach. It follows, deliberately and specifically, the model established by GDPR Article 37 for the Data Protection Officer. The DPO mandate works. The CASS Safeguarding Officer mandate would work for the same reasons.

6.2 The Role of the Certified CASS Safeguarding Officer

Daily Reconciliation	Perform the CASS 15 daily safeguarding reconciliation in accordance with FCA evidence standards; identify all shortfalls, commingling events, and evidence failures.
Audit Trail	Maintain a contemporaneous, timestamped practitioner audit log that can be produced to the FCA on demand.
Escalation	Immediately escalate any RED-flag finding to the Senior Manager Function holder; assess whether the FCA reporting threshold is met and document the assessment.
GDPR Compliance	Handle client financial data in accordance with UK GDPR throughout the reconciliation process; maintain lawful basis documentation and data retention schedules.
Cybersecurity	Operate within the organisation's cybersecurity framework; report any security incident relevant to the reconciliation process.
Professional Independence	Maintain the independence of the compliance function; report findings accurately regardless of commercial pressure; refer clients to legal counsel when advice falls outside the compliance scope.
CPD	Complete annual continuing professional development; maintain certification currency.

6.3 The Qualification Standard

The mandatory CASS Safeguarding Officer appointment should be supported by a prescribed minimum qualification standard, specified by the FCA and met through an accredited professional certification. The qualification must cover:

1. The CASS 15 regulatory framework in full: legislative basis, PS25/12, daily reconciliation mechanics, evidence standards, shortfall and commingling identification, and FCA enforcement.
2. Safeguarding in practice: the operational mechanics of daily reconciliation across individual and pooled account structures, evidence renewal, remediation standards.
3. UK GDPR and data protection law in the CASS context: lawful basis, Article 22 human-in-the-loop requirements, breach notification, data retention.
4. Technology security and system governance: authentication, credential management, secure data handling, threat awareness.
5. Professional ethics and conduct: the five conduct standards applicable to regulated compliance practice — integrity, confidentiality, professional boundaries, competence, and continuous development.
6. Practical assessment: a supervised practical competency examination in which the candidate processes a synthetic client dataset, identifies injected compliance failures, produces a formal determination, and defends their professional judgements under oral examination.

THE CCSL — PROOF OF CONCEPT

The author's own work in developing a structured CASS 15 certification curriculum confirms that this qualification standard is achievable. A rigorous programme covering all six domains listed above — across written examination, case study analysis, supervised compliance project, and oral defence — can be built and delivered. The regulatory framework should provide the mandate that will stimulate the broader market to respond.

6.4 The Human-in-the-Loop Model — Technology and the Professional

The author's experience in building automated CASS 15 compliance technology places him in a position to address, with particular authority, the question of the relationship between the certified professional and the automated tool.

The Sovereign Auditor Machine is designed on a three-tier governance model. At Tier 1, the Machine processes client data against CASS 15 requirements and produces structured analytical findings. At Tier 2, the certified CASS practitioner reviews those findings, applies professional regulatory judgement, and prepares a compliance determination. At Tier 3, the Authorising Director reviews and authorises the determination before it is delivered. Nothing produced by the Machine is delivered without passing through both human review tiers.

This architecture is not merely best practice. It is a legal requirement under GDPR Article 22, which prohibits significant automated decisions unless a qualified human reviews and authorises the output. The certified CASS Safeguarding Officer is the Article 22 human. Without them, the Machine's output is not a compliance determination — it is an unvalidated automated report. With them, it is a legally defensible professional document.

Purpose-built automated compliance technology is an extraordinarily

> *powerful instrument. It can process data at a speed and consistency that no human analyst can match. But it cannot read context. It cannot weigh the significance of an anomaly against the client's broader circumstances. It cannot decide whether to escalate a finding to the FCA. It cannot sign the determination. These are human judgements. The technology exists to support the professional. The professional cannot be replaced by technology. The law should say so.*

6.5 Proportionality — Not Every Firm Needs the Same Thing

A proportionate approach to the mandatory appointment requirement should reflect the volume and complexity of the client money a firm holds. The following framework is proposed for discussion:

Firm Category	Proposed Requirement
EMIs and PIs holding aggregate client money above £5 million	Mandatory appointment of a dedicated, full-time certified CASS Safeguarding Officer; name and certification number registered with the FCA
EMIs and PIs holding £500,000 to £5 million	Mandatory designation of a certified CASS Safeguarding Officer — may be a shared or part-time role within a broader compliance function
EMIs and PIs holding £100,000 to £500,000	Mandatory certification of the individual performing the daily reconciliation — no dedicated appointment required but individual qualification mandatory
EMIs and PIs holding below £100,000	Mandatory completion of FCA-recognised CASS 15 training module by the responsible individual
New authorisations	Evidence of a plan to train or appoint a certified CASS practitioner before client money is first held — condition of FCA authorisation

7. The Opportunity: What a Mandatory CASS Profession Would Create

7.1 Job Creation — Immediate and Substantial

The economic case for a mandatory CASS Safeguarding Officer requirement has received almost no attention in policy discussions. This is a significant omission, because the numbers are compelling.

There are over 900 FCA-regulated EMIs and PIs currently in scope for CASS 15. The FCA authorises new firms continuously. The total regulated population will grow. If the mandatory appointment requirement applies to firms holding more than £500,000 in client money — a conservative threshold — several hundred firms will need to designate a certified CASS Safeguarding Officer immediately. If the requirement applies to all firms in scope, the number rises to over 900 appointments on day one.

Scenario	Estimated Immediate Roles	5-Year Role Projection
Conservative (>£5m client money)	~100 dedicated appointments	~200–300 (accounting for new authorisations)
Moderate (>£500k client money)	~400 designated appointments	~700–1,000
Full (all regulated EMIs and PIs)	900+ appointments	~1,500–2,500 (including new pipeline)

These are not minimum-wage, entry-level positions. A qualified, certified CASS Safeguarding Officer — holding a recognised professional qualification, named and registered with the FCA, and personally responsible for the daily compliance of a regulated firm — would command a salary broadly comparable to a qualified compliance officer, a junior regulatory solicitor, or a practising Data Protection Officer: in the range of £35,000 to £70,000 depending on seniority and firm size. Many would sit significantly above that range in senior roles.

7.2 A New Professional Training and Education Market

A mandatory appointment requirement does not just create practitioner employment. It creates an education and training market. The GDPR DPO mandate stimulated an entire ecosystem — university courses, professional certifications, conferences, and industry bodies — that now generates significant economic activity and employment in its own right. The CASS Safeguarding Officer mandate would do the same.

- Universities would develop and offer accredited CASS compliance modules at postgraduate and CPD level — creating academic employment, research output, and reputational positioning in a high-value regulatory specialisation
- Professional bodies — the ICA, the CISI, the Chartered Institute for Securities and Investment, the Association of Compliance Professionals — would develop specialist membership grades, examination frameworks, and continuing education programmes

- Online training providers would develop and market CASS 15 certification courses to the full regulated population, including smaller firms that cannot afford full-time appointments
- Academic research into CASS compliance governance, the regulation of automated compliance systems, and the intersection of FCA and GDPR obligations would expand — producing scholarship, policy influence, and international academic visibility

7.3 A New RegTech Market Segment

The mandatory CASS Safeguarding Officer requirement, combined with FCA recognition of approved automated compliance tools, would create significant and currently unrealised demand for purpose-built CASS 15 compliance technology.

The data protection technology market — consent management platforms, DPIA tools, breach notification software — was largely created by the GDPR mandate. It now generates billions of pounds globally. The CASS 15 compliance technology market is at an equivalent inflection point. The regulatory demand has been created by PS25/12. What it lacks is the professional mandate that would convert that regulatory demand into a structured commercial market.

- RegTech companies would develop and market FCA-approved CASS 15 compliance tools, certified for use by CASS Safeguarding Officers
- BaaS providers and banking infrastructure firms would embed CASS 15 compliance tooling within their client-facing platforms — making the certified professional's daily task faster and more reliable
- API connectivity between compliance tools, the FCA Register, and banking systems would create a new category of financial data infrastructure with export potential
- The UK would be positioned as the global leader in client money safeguarding technology — a first-mover advantage in a market that will exist in every jurisdiction with equivalent client money obligations

7.4 Improved FCA Supervisory Capacity

The FCA currently has no direct line of sight into who, at each of its 900+ regulated EMIs and PIs, is performing the daily CASS 15 reconciliation, what qualification they hold, or whether their knowledge is current. A mandatory registration requirement — analogous to the ICO's DPO register — would change this entirely.

With a CASS Safeguarding Officer register, the FCA would know, for every firm in scope, who the responsible professional is, what certification they hold, and when that certification expires. Supervisory correspondence on CASS matters could go directly to the qualified practitioner. Thematic reviews could be designed around the practitioner population. An expired or lapsed certification would itself be a supervisory trigger — allowing the FCA to identify non-compliant firms before enforcement action becomes necessary, rather than only discovering the problem after a breach has occurred.

7.5 UK Financial Services Competitiveness

Finally, and most broadly: a mandatory CASS Safeguarding Officer requirement, backed by a recognised professional certification, would strengthen the United Kingdom's competitive position as a domicile for regulated payments and electronic money businesses.

Post-Brexit, the UK's ability to attract regulated fintech activity depends on the quality, clarity, and credibility of its regulatory environment. A regulatory environment that creates obligations without supporting infrastructure is not attractive to sophisticated operators. A regulatory environment that creates obligations and simultaneously creates the professional infrastructure to meet them — with a clear qualification standard, a named professional, and a register — signals institutional seriousness. That is the kind of regulatory environment that attracts investment, headquarters decisions, and talent.

> *The countries that win the competition for regulated financial services are not those with the loosest rules. They are those with rules that are clear, fair, and supported by the professional infrastructure that makes genuine compliance achievable. A mandatory CASS Safeguarding Officer is part of that infrastructure.*

8. Addressing the Objections

8.1 "This Will Be Too Costly for Small Firms"

This objection is predictable and deserves a genuine response. The concern is that imposing a mandatory professional appointment — even at a part-time or certification-only level — will disproportionately burden the small fintechs that are least able to absorb additional compliance costs.

The author's response is threefold. First, the proportionality framework proposed in Section 6.5 is designed precisely to address this concern. Smaller firms are not required to appoint a full-time dedicated professional. They are required to ensure that whoever performs the daily reconciliation holds a defined qualification. A 12–16 week part-time certification programme, completed once, at a cost that is trivial compared to one month of FCA enforcement costs, is not an existential burden.

Second, the alternative — non-compliance — is enormously more expensive. A single FCA fine for CASS 15 breach can exceed £10,000 per breach instance. Across 260 business days, that is potentially £2.6 million per year. An enforcement investigation, even one that does not result in a fine, typically costs firms hundreds of thousands of pounds in legal fees and management time. The 'cost' of a professional qualification is a rounding error by comparison.

Third — and this is the argument the author makes most directly — if a firm truly cannot invest in training one person to comply with the daily obligation it took on when it chose to hold client money, the question must be asked whether that firm is in a position to hold client money at all. CASS 15 exists to protect clients. Client protection costs money. That cost is part of the business of holding client money.

8.2 "No Qualification Exists — You Cannot Mandate What Is Not There"

This objection was accurate at the time PS25/12 was enacted. It is becoming less accurate. The author's own curriculum development work has demonstrated that a comprehensive, rigorous, six-module professional certification covering CASS 15 regulation, safeguarding mechanics, UK GDPR, cybersecurity, and professional ethics can be built, delivered, and assessed. The qualification framework exists. Academic accreditation processes are underway.

More fundamentally, the logic of this objection — that a mandatory standard cannot be announced until the qualification already exists — reverses the correct sequence. Qualifications are created by demand. Demand is created by mandates. The GDPR DPO mandate was announced before a fully developed DPO training market existed. The announcement created the market. The FCA should announce the mandate. The market will respond.

8.3 "SMCR Already Requires Competence"

This objection is technically correct but operationally empty. The SMCR requires Senior Managers and Certification Regime individuals to be fit and proper and to act with competence. It does not specify what competence means in the CASS 15 context. It does not define a minimum training standard. It does not create a qualification. And it does not address the fundamental problem that the Senior Manager needs a trained professional to help them — not merely a theoretical obligation to be competent themselves.

'Be competent' without a defined standard of competence is an aspiration, not a requirement. The CASS Safeguarding Officer proposal converts that aspiration into a requirement — defined, assessed, registered, and verifiable. That is what the SMCR framework currently lacks, and what this proposal would supply.

9. Recommendations

9.1 To the Financial Conduct Authority

7. Issue a Consultation Paper proposing the introduction of a mandatory Certified CASS Safeguarding Officer appointment requirement for all FCA-regulated EMIs and PIs, with a proportionality threshold framework based on the volume of client money held.
8. Specify within that consultation a minimum qualification standard for CASS Safeguarding Officers, requiring coverage of CASS 15 regulation, UK GDPR obligations, cybersecurity governance, and professional ethics — assessed through written examination and practical supervised assessment.
9. Establish a CASS Safeguarding Officer Register, to which every firm in scope must submit the name, qualification, and certification number of its designated officer — modelled on the ICO's DPO register.
10. Engage with academic institutions and professional training providers to recognise accredited CASS qualification programmes — providing the market signal that will stimulate the training ecosystem.
11. Issue supervisory guidance clarifying that holding a recognised CASS Safeguarding Officer qualification will be treated as evidence of reasonable steps under the SMCR — addressing the unjust ambiguity identified in Section 5 of this paper.
12. Publish an approved list of automated compliance tools suitable for use in CASS 15 daily reconciliations — encouraging the adoption of technology that supports, rather than replaces, the certified professional.

9.2 To FCA-Regulated EMIs and Payment Institutions

13. Do not wait for the mandate. Begin training your CASS compliance staff now. The firms that arrive at their first post-7 May 2026 supervisory review with a certified professional and a complete audit trail will be in an entirely different regulatory position from those that do not.
14. Review your Senior Manager Function allocations for CASS responsibility. The named individual must understand what that responsibility entails. If they are not currently equipped with a certified CASS specialist to support them, they are personally exposed.
15. Explore the integration of purpose-built automated compliance tools — particularly those designed on a human-in-the-loop architecture that satisfies GDPR Article 22 requirements and produces a legally defensible audit trail.

9.3 To Academic Institutions

16. Engage with industry partners who have developed CASS 15 curriculum and qualification frameworks. The institution that is first to accredit a CASS Safeguarding Lead qualification will occupy a first-mover position in a market with over 900 firms in immediate need and a growing pipeline of new regulated entities.
17. Develop interdisciplinary CASS compliance research programmes. The intersection of FCA safeguarding law, UK GDPR, cybersecurity governance, and automated

compliance systems governance presents rich and largely unexplored research questions of genuine policy importance.

18. Consider the CASS compliance challenge as a case study in legal-technology intersection: the challenges identified in this paper — how law creates obligations, how technology enables compliance, and why the human professional remains irreplaceable at the centre of both — are teaching material for the next generation of regulatory lawyers and compliance technologists.

10. Conclusion: The Law Must Complete Itself

The Financial Conduct Authority's CASS 15 framework is serious regulation for a serious purpose. Protecting client money — ensuring that when a regulated firm fails, its clients' funds are safe and recoverable — is one of the most important functions that financial regulation performs. PS25/12 strengthens that protection significantly, and the author commends that intent unreservedly.

But serious regulation must be complete regulation. And CASS 15, as it currently stands, is not complete. It creates the obligation but not the professional. It creates the liability but not the qualification pathway. It holds Senior Managers personally accountable but provides them no formally prescribed professional support. It expects competence across three simultaneous regulatory regimes but creates no mechanism for that competence to be reliably acquired.

The author writes this not as a critic of the FCA's objectives, but as a lawyer who understands legal completeness and as the inventor of the Sovereign Auditor Machine who understands what a properly trained professional would use. The Sovereign Auditor Machine can process a client dataset with speed and precision that no manual process can match. But it cannot replace the practitioner who reviews its output, applies professional judgement, takes personal responsibility for the determination, and stands behind that determination when the FCA asks questions. The Sovereign Auditor Machine needs the professional. The professional needs the qualification. The qualification needs the mandate.

The GDPR showed what happens when the law completes itself. A professional was mandated. A qualification market was created. Thousands of jobs were generated. Compliance outcomes improved. The regulator gained a named contact at every qualifying organisation. All of these things happened because the law asked a simple question — who is going to do this? — and answered it.

CASS 15 has not yet asked that question. This paper is the argument for asking it — and the proposal for answering it.

> *A law that creates an obligation without creating the means to comply with it is not complete law. A law that attaches personal liability without providing the professional infrastructure to discharge that liability is not fair law. CASS 15 can be both complete and fair. The policy mechanism exists. The qualification framework exists. The technology exists. The FCA needs only to mandate the professional who brings all three together.*

Olushola Oke-Daniel

Barrister and Solicitor, Supreme Court of Nigeria

Founder & Director, AFC Fintech Ltd

Contributor: Dr Kolawole Oyekan
Chief Regulatory Director, AFC Fintech Ltd

March 2026

References and Regulatory Sources

Primary Regulatory Sources — UK

1 Financial Conduct Authority, Policy Statement PS25/12, 'Safeguarding Review: Changes to our rules for payments and e-money firms' (FCA, 2025).

2 FCA Handbook, CASS 15: Client Money Safeguarding for Payment Services and Electronic Money Firms.

3 Financial Services and Markets Act 2000 (as amended) — FCA supervisory and enforcement powers.

4 Senior Managers and Certification Regime — FCA Supervisory Framework and Policy Statements.

5 Electronic Money Regulations 2011 (SI 2011/99), as amended.

6 Payment Services Regulations 2017 (SI 2017/752), as amended.

Data Protection and Privacy Law

7 Regulation (EU) 2016/679 (General Data Protection Regulation), as retained in UK law ('UK GDPR') under the European Union (Withdrawal) Act 2018.

8 Data Protection Act 2018 (UK).

9 Information Commissioner's Office, 'Guide to the UK GDPR — Data Protection Officers' (ICO, current edition).

10 Article 37, UK GDPR — Designation of the Data Protection Officer.

11 Article 22, UK GDPR — Automated individual decision-making, including profiling.

Cybersecurity and Operational Resilience

12 Network and Information Systems (NIS) Regulations 2018 (UK).

13 FCA, 'Operational Resilience: Impact tolerances for important business services', PS21/3 (FCA, March 2021).

14 Regulation (EU) 2022/2554 — Digital Operational Resilience Act (DORA) — UK equivalence framework under consideration.

15 National Cyber Security Centre, 'Guidance for financial sector: secure systems and access management' (NCSC, current edition).

Academic and Professional Qualification Sources

16 Oke-Daniel, O., 'AFC Certified CASS Safeguarding Lead (CCSL) Programme Specification', AFC Fintech Ltd (March 2026) — submitted for academic partnership consideration.

17 Quality Assurance Agency for Higher Education, UK Quality Code for Higher Education.

18 UK Framework for Higher Education Qualifications (FHEQ) — Level 7 descriptor.

19 International Association of Privacy Professionals, 'Global Privacy Professionals and DPO Report 2025' (IAPP, 2025).

20 Financial Conduct Authority, 'Approved Persons Regime Review and the Introduction of the Senior Managers and Certification Regime' — FCA Consultation Papers CP14/13, CP15/22, and related Policy Statements.

Contact

Author	Olushola Oke-Daniel, Barrister & Solicitor, Supreme Court of Nigeria
Contributor	Dr Kolawole Oyekan
Organisation	AFC Fintech Ltd
Email	olushola@fintechafc.co.uk

Telephone	07473 735 005
Regulatory Anchor	FCA PS25/12 · CASS 15 · Effective 7 May 2026