GUIDE

# How to meet the expanded non-financial misconduct rules with Global Relay

A practical guide for non-bank compliance, legal, and HR teams at firms subject to the Financial Services and Markets Act 2000.

Integrity | Reputation | Control

globalrelay.com

# About this guide

Starting September 1, 2026, roughly 37,000 non-bank firms subject to the Senior Managers and Certification Regime (SMCR) fell in scope of the Financial Conduct Authority's (FCA's) non-financial misconduct (NFM) rules. With this change, serious bullying, harassment, and violence (among other offenses) breach the FCA's Conduct Rules (COCON), making NFM a compliance issue for non-banks.

Many firms had been amending policies and creating "seriousness" frameworks before the deadline took effect. They also focused on training staff members to understand what the new rules entail. This work is vital, but the FCA's attention will soon extend beyond policy and training toward evidence.

> **Closing out its policy work in PS25/23, the regulator was explicit that it "will now focus on how firms are tackling [NFM] in practice." FCA CEO Nikhil Rathi said that the FCA expects firms to have effective systems in place to identify and mitigate risks more broadly than before, particularly when it comes to employee conduct—not just relevant policies.**

This shifts the burden from documentation to evidence. And evidence is notoriously a data problem rather than a policy problem. Does your firm capture, store, and monitor the communications data necessary in the event of NFM?

**To clarify what's happened and what firms need to do, this guide covers:**

1. **The evolution of NFM rules** from 2018 to present
2. **What in-scope firms are expected to do**/ their practical obligations
3. **How to meet the new rules** by capturing, detecting, evidencing, and investigating NFM in one place with Global Relay

For a primer on the NFM changes, start with our essential guide to the NFM rules extending to SMCR firms and our 10-step readiness checklist.

# The evolution of NFM rules

Although NFM may be a new concept for non-banks, it's been building as a supervisory theme for nearly a decade, especially for U.K. regulators. Here's a high-level timeline.

## 2018 FCA says "misconduct is misconduct"

Following the FCA's correspondence with the Women and Equalities Committee, the regulator set a position that it's consistently maintained: "non-financial misconduct is misconduct, plain and simple." This laid the foundation for the idea that NFM should be given equal weight and attention as what financial misconduct receives.

## 2023 A formal framework is proposed

In September 2023, the FCA published CP23/20 "Diversity and inclusion in the financial sector—working together to drive change," which proposed a formal regulatory framework covering diversity, inclusion, and NFM. The publication attracted significant industry response, and the diversity and inclusion elements were ultimately set aside. NFM, however, wasn't.

## 2024 Firms are compelled to provide NFM information

In February 2024, the FCA issued a formal Notice to Provide Information to 1,028 regulated wholesale financial services firms. Under Section 165 of the Financial Services and Markets Act 2000 (FSMA), the FCA compelled firms to provide data about in-house incidents of NFM. After receiving the letter, 96% of firms replied, and their responses showed incidents of increasing NFM. This data directly influenced the subsequent Consultation Paper and final NFM framework.

## 2025 NFM scope is confirmed

In July 2025, **Consultation Paper CP25/18** confirmed the FCA's intention to extend COCON to explicitly capture serious bullying, harassment, and violence across all SMCR firms. This essentially closed the gap between how the FCA treats non-banks and banks, which had long been in scope.

The FCA's own survey found that 95% of respondents wanted further guidance on how to apply the rules. The final **Policy Statement PS25/23** responded with suggested examples, a seriousness framework, and a scenario table under COCON 1.3.7G with clarifying examples of what conduct was in scope and out of scope.

## 2026 NFM rules take effect

Beginning September 1, 2026, the extended rules apply to non-banks.

# Why is NFM in the spotlight?

The FCA has focused on NFM from more of a risk detection and mitigation standpoint rather than to directly address employee welfare.

## NFM points to potential misconduct

Regulators rarely first catch misconduct, whether financial or otherwise. Instead, it's typically caught by colleagues. A work culture that tolerates harassment teaches people to not speak up about issues and often indicates wider business risk.

**As the FCA highlighted: "Too often where we see poor market conduct, or consumers being failed by financial services firms, we find cultural failure within firms. One of the clearest warning signs of a failing culture is non-financial misconduct—behaviors such as bullying and sexual harassment—going unchallenged."**

## Groupthink

Exclusionary behavior keeps diverse perspectives out of decision-making, which is a known risk factor. On a commercial and reputational level, it's clear why NFM is not only an HR issue but also a compliance issue. The FCA's expectations look far more like risk controls than they do employee policies.

# What firms need to do

The new NFM rules outline five key obligations.
Each places a data-based dependency on compliance teams.

### 1. Capture all business communications to meet the extended COCON scope

Previously, conduct rules for non-banks were generally attached to regulated activities. COCON now extends to bullying, harassment, and violence (among other things) directed at any colleague, provided there's a sufficient work-related link. The FCA has updated its handbook with a series of example scenarios for the new rules.

**Some of the in-scope scenarios include:**

- Conduct on firm premises
- Remote interactions over Zoom and Slack
- Offsite events
- Social media posts from work-issued devices

**Data dependency:** If your firm isn't capturing all business communications data, it won't have full oversight of the channels where NFM may take place. This means you could be missing crucial evidence in the event of a complaint or investigation.

## 2. Document that your firm judged a situation with appropriate seriousness

Under the new rules, the FCA will be evaluating whether firms used professional judgment to determine the "seriousness" of an action. The regulator has deliberately avoided defining "seriousness" on the basis that firms are best suited to assess individual circumstances. Relevant factors include the purpose behind the conduct and whether a pattern of behavior exists.

**Data dependency:** Patterns form over time. Detecting them requires historical evidence and cross-channel context to piece together behaviors. A single message rarely establishes a pattern, so a complete, tamper-proof archive is essential.

## 3. Hold management accountable

A manager can breach COCON Rule 2 (due skill, care, and diligence) by failing to take reasonable steps to prevent harassment or by failing to take complaints seriously. This is not a strict liability, but it creates personal exposure if a manager knew, or should have known, that NFM was taking place.

**Data dependency:** With data monitoring tools, "should have known" may now be assessed against what a firm's technology and controls were able to surface. Weak detection because of outdated tools increases individual exposure, as well as firmwide reputational risk.

## 4. Perform FIT assessments

NFM history is now material to fitness and propriety (FIT). Disciplinary outcomes and conduct concerns need to feed into annual FIT reviews.

**Data dependency:** For FIT reviews to be complete and accurate, information must move seamlessly between HR and compliance. To ensure this happens, all teams should have access to one single data source.

## 5. Report serious NFM

Firms must notify the FCA of serious NFM that meets the reporting threshold. Every decision must be documented, including when a decision was made **not** to notify.

**Data dependency:** A defensible decision log must be comprehensive and show all underlying and historical records.

# How to meet the NFM rules with Global Relay solutions

We approach NFM through four connected capabilities on a single platform: capture everything in scope, detect risk in communications, evidence what you did about it, and investigate it defensibly.

## Capture communications: Close the channel gap first

Global Relay Connectors allow you to capture the channels where work-related conduct actually happens.

If you're not capturing the communications channels that employees use for business, you're missing vital evidence of potential NFM. Your ability to detect misconduct will therefore depend on your data's completeness:

- **Enterprise collaboration**
  Our connectors comprehensively capture text, voice, and video, so nothing gets missed. For example Microsoft Teams, Slack, Zoom, Webex, Instant Bloomberg, Symphony, Telegram, and Google Workspace.
- **Mobile and text**
  And carrier-level capture through Vodafone, O2, and Verizon brings mobile messaging into scope.
- **AI Communications**
  We even have connectors for ChatGPT Enterprise, Microsoft Copilot, and Claude to compliantly cover AI interactions.
- **Custom SMTP**
  When a channel has no off-the-shelf connector, the Global Relay Open Connector API supports any source using a standardized format that we can build custom integrations from.

On ingestion, our connectors automatically normalize, group, dedupe, and archive your data. This allows for holistic channel capture, streamlined search, and the ability to analyze all business communications in one place across business functions.

## Detect risk: Go beyond keyword matching

Global Relay Surveillance applies a multilayered approach: standardization and enrichment, transcription and translation, noise reduction, risk identification, and investigation and reporting.

Most of these capabilities are directly relevant to NFM:

- **Contextual risk identification**
  Rather than matching individual terms, our large language model applies a structured chain of thought process that reviews messages in full context before making an alert decision. This allows the system to detect misconduct where keyword lists can't, such as when conduct is ambiguous, is context dependent, or contains coded language.
- **Sentiment analysis**
  Unlike lexicon-based detection, sentiment analysis looks at emotional context in messages to decipher tone and power imbalances, which surfaces risks, including harassment.
- **Multilingual and voice coverage**
  Our solution detects and translates multiple languages. Non-English voice calls are automatically transcribed into searchable text in English, so nothing gets missed.
- **Noise reduction that improves reviewer attention**
  False positives are historically a huge barrier to compliance by taking the focus away from alerts that matter. Global Relay's rules-based filtering, approved sender and content lists, spam detection, and thread deduplication capabilities drastically cut down on false-positives that cause reviewers to stop reading alerts carefully. For NFM, this is a huge detection benefit.

## Provide evidence: Build a defensible record

Global Relay Archive stores all your communications data in one secure, tamper-proof repository.

It allows compliance teams to deliver defensible evidence in instances of alleged NFM via the following features:

- **Gold-copy preservation and constant integrity checks**
  Each communication is saved once as a single authoritative record with continuous validation that keeps records complete and unaltered throughout the retention lifecycle.
- **A full audit trail**
  All access, search, export, and administrative actions are recorded and time-stamped to maintain chain of custody, which supports investigations as well as any later challenges to how an investigation was handled.
- **Retention policy management**
  Apply schedules to jurisdictions, entities, and business units. This keeps NFM findings available for a longer period than routine records, so they can be referenced for regulatory purposes.

## Investigate and report: From alert to regulatory notification

Once an allegation is made, the clock starts on substantiation, FIT input, reference disclosure, and the FCA Handbook's SUP 15 decision.

- **Identity-aware search**
  Identity-aware search works from custodian profiles rather than individual addresses and automatically includes every alias and communication identity associated with someone. That way, an investigation never misses an individual's mobile number, Bloomberg identity, or legacy address.
- **Find communication across channels**
  Unified cross-channel search spans email, messaging, voice, mobile, and collaboration platforms from one normalized archive.
- **Defensible legal holds**
  Legal hold controls preserve records by custodian, domain, case, and dynamic criteria and are independent of retention schedules.
- **Complete audit trails**
  Defensible export produces records in accepted evidentiary formats, backed by an object change log that records every action taken during a workflow.

Together these capabilities mean that firms can quickly and completely respond to NFM investigations with defensible and documented outcomes.

## Govern: Bridge HR and compliance without collapsing controls

Sharing consistent data between departments is a well-known challenge. Whether it's between recordkeeping and surveillance teams or compliance and HR, a lack of merged data leads to protracted processes and erroneous outcomes.

- **Workspaces for Legal, HR and Compliance**
  Global Relay Archive supports ring-fenced workspaces, which maintain separate compliance, legal, HR, and IT workflows while all drawing from the same archive. This provides a practical way to deliver a unified escalation workflow that the rules now require.
- **Access control dependant on roles**
  You may also need to meet Data Protection Impact Assessments (DPAIs) based on the proportionality argument. Being able to demonstrate that HR reviewers see only what their role requires on sanctioned business channels with every access logged, is a substantially stronger position than blanket access or no access at all.

# FCA obligations and Global Relay's solutions

| FCA obligation | Global Relay's solution |
| --- | --- |
| **Extend COCON scope across work-related channels**<br>Complete capture of channels where misconduct occurs | ✓ **Channels capture and Global Relay App**<br>Compliant WhatsApp, IM, voice, and text on BYOD and corporate devices |
| **Document seriousness assessments**<br>Detect patterns, tone, and intent | ✓ **Communications monitoring**<br>Featuring chain of thought contextual analysis, sentiment analysis, and 130+ risk indicators |
| **Show "reasonable steps" taken**<br>Surface issues early enough for managers to act | ✓ **Communications monitoring**<br>With contextual risk alerts and activity dashboards |
| **Make FIT assessments that include NFM history**<br>Provide structured information flow between HR and compliance | ✓ **Global Relay Archive**<br>With ring-fenced workspaces and role-based access controls |
| **Notify and log decisions per SUP 15**<br>Maintain a defensible record of every decision, including non-notification | ✓ **Global Relay Archive**<br>Which offers a full audit trail, transparent alert explanations, legal hold functionality, and defensible exports with object change logs |
| **Provide evidence that controls actually work**<br>Run reports that a supervisor can inspect | ✓ **Reconciliation and compliance reporting**<br>Proof of review, policy coverage, supervised users, and reviewer activity |

# Talk to us about your NFM control framework

We've been building communications compliance infrastructure for over 25 years.

Our developer team is more than 300 experts strong.

Global Relay is a Leader in the Gartner® Magic Quadrant™ for Digital Communications Governance and Archiving Solutions.

**We provide:**

- ISO 27001 certification
- SOC 2 Type II attestation
- 24/7/365 support from London, New York, and Vancouver

**To discuss how we can help you meet the FCA's expanded NFM rules, → get in touch**

GARTNER and MAGIC QUADRANT are registered trademarks of Gartner, Inc. and/or its affiliates; Gartner does not endorse any vendor depicted in its research publications.

Integrity | Reputation | Control

North America: +1 866 484 6630
Europe: +44 20 3206 1850

**globalrelay.com**