MEMA

CONSULTANTS

REGULATORY INSIGHT

FCA PS26/2: New Incident Reporting Hits Almost Every Firm

The FCA's new operational incident and third-party reporting regime reaches nearly every…

Insight. Clarity. Confidence.

FCA PS26/2: New Incident Reporting Hits Almost Every Firm

The FCA's new operational incident and third-party reporting regime reaches nearly every authorised firm from March 2027, here's what small and medium firms must do now.

MEMA Consultants · Regulatory Insight · Published 23 August 2026

Why this is the development to watch

Over the past year the FCA has published a lot: motor finance redress work, Consumer Duty follow-up letters, AML "Dear CEO" letters, wealth management supervisory correspondence, and a package of AIFM reforms. Most of these land on specific sectors. One development lands on almost everyone.

On 18 March 2026 the FCA published Policy Statement PS26/2, "Operational incident and third party reporting," alongside the Prudential Regulation Authority's parallel PS7/26 (Operational resilience: Operational incident and third-party reporting) and SS1/26 (Operational resilience: Incident reporting), both in force on the same date, and finalised guidance from the FCA (FG26/3 on operational incidents and FG26/4 on material third party arrangements) [1][2][3]. The Bank of England published a parallel statement the same day [8]. This followed Consultation Paper CP24/28, published in December 2024, on which the consultation closed on 13 March 2025 [4].

The reason this is the single highest-impact item for small and medium firms is scope. The FCA's own summary of the policy states that operational incident reporting applies to "all firms with Part 4A permission," plus payment service providers, UK Recognised Investment Exchanges, registered trade repositories and registered credit rating agencies [1][4]. Part 4A permission is the standard FSMA authorisation that essentially every FCA-regulated firm holds. That means payments and e-money firms, cryptoasset firms with relevant permissions, consumer credit firms, investment firms, and IFAs are, in principle, all in scope for at least the "standard" reporting tier. This is not a niche prudential change for banks and insurers; it is a new, mandatory reporting obligation reaching down into small firms that have never had to report operational incidents to the FCA in this way before.

The rules do not bite immediately. They come into force on 18 March 2027, giving firms a 12-month preparation window from publication [1][2][3][4]. That means the practical planning work, building an incident classification process, mapping third-party dependencies, assigning ownership, needs to happen now, in the second half of 2026, not in the first quarter of 2027.

What the FCA is actually requiring

The regime has two separate strands. Firms need to work out which one (or both) apply to them.

1. Operational incident reporting

An "operational incident" is defined as a single event, or a series of linked events, that disrupts a firm's operations and either disrupts the delivery of a service to external end users, or affects the availability, authenticity, integrity or confidentiality of information or data relating to those users [5][6]. This is a broad, principles-based definition rather than a narrow technical one, it is intended to capture cyber incidents, IT outages, data breaches and third-party service failures alike, not just classic "systems down" events.

Firms must report where they reasonably believe an incident could cause, per the FCA's threshold:

- Intolerable levels of harm to consumers from which those consumers cannot easily recover;
- A risk to the safety and soundness of the firm or other market participants; or
- A risk to market stability, integrity, or confidence in the UK financial system [6].

Two reporting tiers apply:

Tier	Who	Initial report	Ongoing/final report
Standard	Most FCA solo-regulated firms	Single, short submission via FCA Connect	No mandatory updates
Enhanced	Enhanced scope SM&CR firms, banks, designated investment firms, building societies, Solvency II firms, CASS large firms, PSPs, UK RIEs, registered trade repositories, registered credit rating agencies	As soon as practicable, and in any event within 24 hours of determining a threshold is met	Updates where there is a significant change in circumstances; final report within 30 working days of resolution, extendable to 60 working days where that is impracticable

Read the 24 hours as a backstop rather than a target. The obligation is to report as soon as practicable once the firm reasonably believes a threshold is met, and 24 hours is the outer limit on that, not an investigation window to be used in full.

Payment service providers separately keep a shorter clock: major operational and security incidents must be reported within four hours of first detection. This is a pre-existing obligation under the Payment Services Regulations 2017 rather than something PS26/2 introduces, so it sits alongside the new regime rather than being a second tier within it [5][6].

One genuinely helpful design choice: firms make a single submission through FCA Connect regardless of which regulator(s) the report is ultimately relevant to, removing the old problem of firms filing near-duplicate reports to the FCA, PRA and Bank of England separately [1][3][6].

2. Material third party (MTP) reporting and register

This strand has a narrower scope. It applies to enhanced-scope SM&CR firms, banks and building societies, PRA-designated investment firms, Solvency II firms, CASS large firms, UK Recognised Investment Exchanges, authorised electronic money and payment institutions, and consolidated tape providers [1][6]. Enhanced-scope SM&CR generally means firms with assets under management around

£50 billion or more (calculated on a three-year rolling average) [6], so most genuinely small firms will sit outside this strand, but mid-sized and growing payments/e-money institutions should check carefully, since authorised EMIs and payment institutions are named explicitly.

A "material third party arrangement" is one whose disruption or failure could cause severe harm to the firm's clients, threaten UK financial system stability, or cast doubt on the firm's ability to meet its FCA threshold conditions [1][5]. Examples the guidance treats as normally material include cloud and data-centre services, cyber security services, and services underpinning a firm's "important business services." Consultancy, legal services, utilities and office supplies are not generally expected to be material [6].

Firms in scope must:

- Notify the FCA of new material third-party arrangements and significant changes to existing ones, early in the decision-making process and before commitments are finalised [6];
- Maintain a register of all material third-party arrangements, accurate as at 31 December of the previous year, and submit it annually within 90 calendar days of the FCA opening the reporting window [5][6].

Intra-group arrangements are exempt from notification where the service is provided wholly within the group with no external dependency, and third-country branches are excluded from the notification obligation [6]. Law firm summaries of the policy also report an exemption for credit unions with assets below £50 million; that figure comes from secondary commentary rather than a direct read of the FCA text, so credit unions near the threshold should confirm it against the instrument itself [7].

Rule references

The FCA has made these changes principally through Principle 11 of its Principles for Businesses and through SYSC 15A (Operational resilience) [4][5], with a new FCA instrument (FCA 2026/6, "Notification of Third Party Arrangements and Operational...") amending the Handbook, effective 18 March 2027 [9]. On the PRA side, the parallel material sits in a new PRA Supervisory Statement SS1/26 and an updated SS2/21 [6].

Why the FCA is doing this

The FCA's stated reasoning, as reported in its policy materials, is that operational disruption harms consumers and the wider sector, and that a growing share of the incidents reported to the FCA originate at third parties as firms become increasingly reliant on externally supplied services (cloud hosting, payment rails, KYC/AML tooling, core banking platforms) [4][7]. The policy is explicitly framed as a response to "rising threats to operational resilience" and the increasing concentration of critical functions in a small number of third-party providers [7]. This sits alongside, but is distinct from, the separate "critical third parties" regime for the small number of providers designated as critical to the sector as a whole; PS26/2 is about what regulated firms themselves must report, not about direct FCA oversight of the tech vendors.

Who is genuinely in scope, in plain terms

Firm type	Operational incident reporting	MTP register/notification
Small payments/EMI firm	Yes (standard tier, unless it meets enhanced criteria)	Only if authorised EMI/PI and materiality threshold met
Cryptoasset firm with Part 4A permission	Yes (standard tier)	Generally no, unless enhanced-scope criteria met
Small/medium consumer credit firm	Yes (standard tier), if it holds Part 4A permission	Generally no
Small/medium investment firm or IFA	Yes (standard tier)	Generally no, unless CASS large or enhanced SM&CR
Payment service provider (non-PSD account info/payment initiation exempt)	Yes, with 4-hour initial detection clock in enhanced tier	Yes, named explicitly

Firms that are consumer credit-only or investment/advice firms without Part 4A permission (a small minority) should check their authorisation basis carefully, since the incident-reporting obligation is tied to permission type, not firm size.

Common failure modes to plan against

1. **Treating this as an IT problem, not a governance one.** The definition of "operational incident" explicitly covers data confidentiality, integrity and authenticity issues, not just outages. A data breach, a mis-sent client file, or a third-party payroll provider losing personal data can all trigger the reporting duty. Firms that route this solely through an IT helpdesk process will miss the threshold judgement, which needs compliance and senior management involvement.

2. **No pre-agreed threshold test.** The FCA's threshold language ("intolerable harm," "risk to safety and soundness," "risk to market stability") is judgement-based. Firms that wait until an incident happens to work out whether it meets the bar will report late, or not at all. The action item now is to build a simple decision tree, mapped to the firm's own products and client base, that a duty manager can apply within hours of first learning of an incident.

3. **Third-party mapping gaps.** Even firms outside the MTP register requirement should map their key third-party dependencies now, because an incident originating at a supplier (cloud host, payments processor, core banking platform, outsourced KYC provider) still triggers the firm's own incident-reporting duty. If a firm does not know which suppliers underpin which "important business services," it cannot make the reporting judgement quickly.

4. **Assuming the 12-month runway means nothing to do until early 2027.** Building and testing an incident classification and escalation process, briefing the board, and updating

outsourcing/operational resilience policies (which most small and medium firms already hold under the existing SYSC 15A operational resilience rules) takes longer than firms expect, particularly where board sign-off and staff training are involved.

5. **Missing the single-portal advantage.** Firms that are dual- or triple-regulated (FCA/PRA/BoE) should note the single-submission design is meant to reduce duplicate reporting. Compliance teams should update internal escalation procedures to route through the new single FCA Connect submission rather than legacy separate processes.

Practical action list for compliance officers now

- Confirm your firm's authorisation basis (Part 4A permission, PSP status, EMI/PI authorisation) and map it against the scope tables above to establish standard vs enhanced tier, and whether the MTP strand applies.
- Update, or create, an operational incident policy that defines internal escalation triggers mapped to the FCA's three harm categories (consumer harm, firm/market participant safety and soundness, market stability/integrity).
- Identify who in the firm will own the reporting decision and the FCA Connect submission, and ensure this sits with someone senior enough to make a fast judgement call, not just an IT lead.
- Build or refresh a third-party/outsourcing register now, even if the formal MTP register obligation does not apply to you, because you will still need to identify quickly whether an incident originated with a supplier.
- Review existing SYSC 15A operational resilience work (important business services, impact tolerances) and check it lines up with the new incident definitions, since the two frameworks are meant to work together.
- Diarise a board or senior management briefing before the end of 2026, so governance and budget for any new reporting tooling or process is in place well before the 18 March 2027 go-live.
- Watch for FCA supervisory engagement and further guidance in the run-up to go-live; the FCA has said it will engage with firms during the transition period [3].

Sources

1. FCA, "PS26/2: Operational incident and third party reporting," fca.org.uk, https://www.fca.org.uk/publications/policy-statements/ps26-2-operational-incident-third-party-reporting, publication date (18 March 2026), scope description ("all firms with Part 4A permission" etc.), MTP scope list. Accessed 20 August 2026.
2. Bank of England / PRA, "PS7/26 – Operational resilience: Operational incident and third-party reporting," https://www.bankofengland.co.uk/prudential-regulation/publication/2026/march/operational-incident-and-third-party-reporting-policy-statement, confirms parallel PRA/BoE publication on 18 March 2026 and PRA scope (banks, building societies, PRA-designated investment firms, Solvency II firms, Lloyd's/managing agents). Accessed 20 August 2026.
3. Global Regulation Tomorrow (Norton Rose Fulbright), "FCA, PRA and BoE issue Policy Statements on operational resilience," https://www.regulationtomorrow.com/2026/03/fca-pra-and-boe-issue-policy-statements-on-operational-

resilience/, confirms 18 March 2027 implementation date, 12-month preparation period, single-portal design, reduced-question standard form for solo-regulated firms/credit unions, FCA engagement commitment. Accessed 20 August 2026.

4. Macfarlanes, "Operational Incident and Third Party Reporting: The FCA's new framework under PS26/2," https://www.macfarlanes.com/insights/102mqoq/operational-incident-and-third-party-reporting-the-fcas-new-framework-under-ps2/, CP24/28 reference, SYSC 15A reference, operational incident definition, register "as of 31 December" and 90-day submission window, practical steps. Accessed 20 August 2026.
5. Sidley, "UK Operational Incident and Third-Party Reporting Rules: What Firms Should Do Now," Data Matters Privacy Blog, https://datamatters.sidley.com/2026/04/16/uk-operational-incident-and-third-party-reporting-rules-what-firms-should-do-now/, reporting timeframes (24hr/4hr/30-60 working days), MTP definition and examples (cloud, cyber services vs consultancy/legal/utilities), enhanced-scope SM&CR £50bn AUM threshold, Payment Services Regulations 2017 reg. 99 reference. Accessed 20 August 2026.
6. Sidley (same article as 5), used again for the detailed scope table (enhanced vs standard tier firm types), notification timing ("early in decision-making"), intra-group and third-country branch exemptions. Accessed 20 August 2026.
7. Global Financial Regulatory Blog (Skadden), "UK Regulators Finalise Policy on Operational Incident and Third-Party Reporting," https://www.globalfinregblog.com/2026/03/uk-regulators-finalise-policy-on-operational-incident-and-third-party-reporting/, FCA rationale (harm from disruption, third-party origin of incidents, growing reliance on external services), credit union £50m asset exemption. Accessed 20 August 2026.
8. Bank of England PS7/26 page (see source 2), confirms same-day parallel publication.
9. FCA Handbook instrument, "FCA 2026/6 Notification of Third Party Arrangements and Operational..." https://api-handbook.fca.org.uk/files/instrument/GLOSSARY-SYSC-SUP/FCA%202026/6-2027-03-18.pdf, confirms instrument number and 2027-03-18 effective date encoded in the file name/path. Accessed 20 August 2026 (file located via search; full text not parsed).
