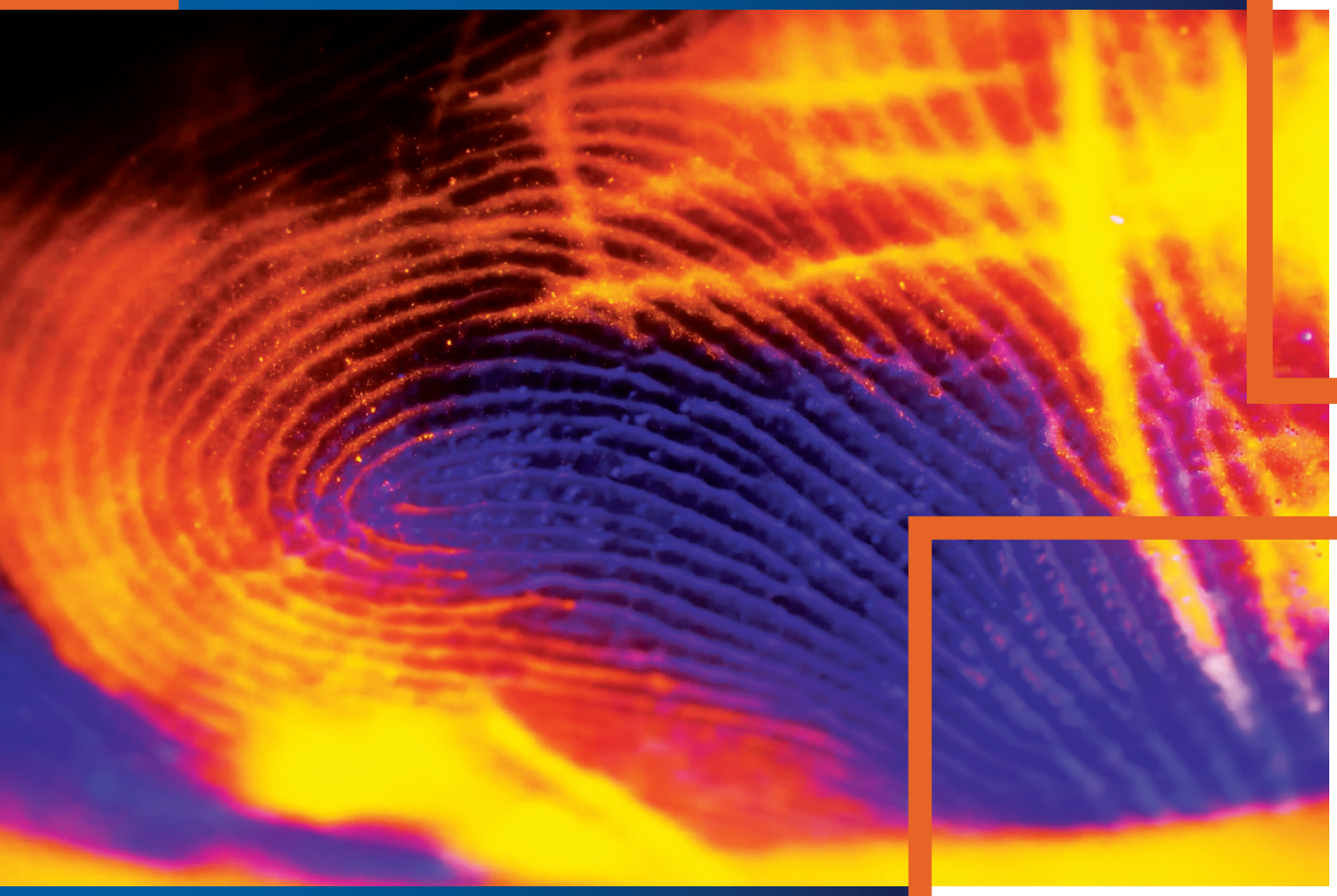
International Comparative Legal Guides

Fintech 2026

A practical cross-border resource to inform legal minds

10th Edition

Contributing Editors:
David Ives, David Shone & James Cook
Slaughter and May



glg Global Legal Group

iclg

Expert Analysis Chapter

1 Operational Resilience: Reporting Rules Herald the Next Chapter for the Financial Sector
David Shone, Natalie Donovan & Emily Bradley, Slaughter and May

Q&A Chapters

5 **Australia**
Peter Reeves, Emily Shen & Billy Elsum, Gilbert + Tobin

17 **Austria**
Mag. Johannes Frank & Mag. Christoph Renner, Herbst Kinsky Rechtsanwälte GmbH

22 **Bahamas**
Christel Sands-Feaste, Portia J. Nicholson & Julia Koga da Silva, Higgs & Johnson

28 **Bahrain**
Saifuddin Mahmood, Mohamed Altraif & Yasmeen Jawahery, Hassan Radhi & Associates

35 **British Virgin Islands**
Andrew Jowett & Patrick Gill, Appleby (BVI) Limited

40 **Cyprus**
Demos Katsis, Katsis LLC

44 **Denmark**
Tue Goldschmieding, Morten Nybom Bethe & David Telyas, Gorrissen Federspiel

51 **Egypt**
Ibrahim Shehata, Hesham Kamel, Safa Rabea & Omar Selim, Shehata & Partners Law Firm

59 **France**
Bena Mara & Félix Marolleau, Bredin Prat

66 **Ghana**
Gregory Kwadwo Asiedu, Kwesi Dadzie-Yorke, Nii Tetteh-Djan Abbey & Pearl Mawuse Jackson, Asiedu & Yorke

75 **Greece**
Marios D. Sioufas & Aikaterini Gkana, Sioufas & Associates Law Firm

83 **Hong Kong**
Vincent Chan, Slaughter and May

99 **India**
Anu Tiwari, Hamraj Singh, Divyam Garg & Keerti Singh, Cyril Amarchand Mangaldas

110 **Ireland**
Sarah Cloonan & Katie Keogh, Mason Hayes & Curran LLP

120 **Isle of Man**
Claire Milne & Katherine Garrood, Appleby (Isle of Man) LLC

125 **Japan**
Atsushi Fukasawa, Ryohei Kudo, Minako Ikeda & Nobuyuki Kaneki, Iwata Godo

132 **Malaysia**
Timothy Siaw, Krystle Lui & Hon Yee Neng, Shearn Delamore & Co.

141 **Malta**
Dr. Cherise Abela Grech & Dr. Ian Gauci, GTG

147 **Netherlands**
Mariska Enzerink, Pete Lawley, William Slooff & Lisa Brouwer, De Brauw Blackstone Westbroek

158 **Philippines**
Enrique V. Dela Cruz, Jr., Jay-R C. Ipac & Terence Mark Arthur S. Ferrer, DivinaLaw

167 **Portugal**
Hélder Frias, Uría Menéndez

176 **Singapore**
Kenneth Pereire, Lin YingXin & Sreya Violetta Sobti, KGP Legal LLC

183 **Spain**
Leticia López-Lapuente & Isabel Aguilar Alonso, Uría Menéndez

193 **Switzerland**
Daniel Flühmann & Peter Ch. Hsu, Bär & Karrer

203 **Taiwan**
Ken-Ying Tseng, Hsin-Hsin Cheng, Yi-Mei Pan & Leo Hsu, Lee and Li, Attorneys-at-Law

210 **Thailand**
Rapinnart Prongsiriwattana, Chositar Daecharux, Daoanong Pongkhao & Masitorn Boonserm, Weerawong, Chinnavat & Partners Ltd.

217 **United Arab Emirates**
Abdus Samad & Luca Rayes Palacín, Afridi & Angell

223 **United Kingdom**
David Ives & David Shone, Slaughter and May

232 **USA**
Brian S. Korn & Bernhard Alvine, Manatt, Phelps & Phillips, LLP

Operational Resilience: Reporting Rules Herald the Next Chapter for the Financial Sector


David Shone


Natalie Donovan


Emily Bradley

Slaughter and May

On 18 March 2026 the FCA, PRA and Bank of England (Bank) published policy statements introducing new requirements and expectations for the reporting of certain operational incidents, and expanding the scope of existing data collections on third-party arrangements.[1] These measures, which follow a package of consultation papers published back in December 2024, are the latest in a series of initiatives to support the operational resilience of the UK financial sector. In particular, they are hot on the heels of the introduction of a new oversight regime for critical third parties to the financial sector (CTPs) in January 2025, which should go live this year.[2]

The new reporting framework responds to a financial sector that is increasingly interconnected, complex and dynamic, and a climate where threat actors are attacking firms (and the third parties they rely on) with greater frequency and sophistication. Firms increasingly rely on third parties to deliver their services, which are now supplying their services by means of transformative technological innovations like AI. Fintech is at the heart of this story, as market participants race to find better ways of interacting with customers via apps and digital platforms, optimise data (including through agentic AI), and build innovative financial products and payment rails using blockchain technology. Against this backdrop, the regulators need to understand how firms are using third parties to effectively supervise their operational resilience.

Incident reporting and third-party reporting, working in tandem, are expected to give the regulators a clearer picture of linkages and dependencies in the sector, enabling appropriate supervision. The data firms submit will help the regulators triage incidents at pace and respond appropriately.

There is a fair amount of regulatory material to digest here; in addition to their respective policy statements and templates, the FCA has published guidance and the Bank and PRA have published supervisory statements to accompany the new rules. In this chapter, we highlight the headlines and key points of interest, focusing on the FCA and PRA materials (and flagging that financial market infrastructures should further review the Bank's materials).

Incident Reporting

The new incident reporting framework – which applies to all authorised firms including payment service providers (PSPs) – requires firms to report basic information promptly in a structured format to help the regulators triage incidents across the sector.

Previously, the regulators complained that they received inconsistent reporting from firms on the types and severity of incidents that occur. The regulators have now created a standardised incident reporting process through a single portal, so all firms make one submission regardless of which regulator(s) a report is for. Firms are divided into two groups: 'standard' reporting for the majority of FCA solo-regulated firms (who make a single short report); and 'enhanced' for a smaller subset, including dual-regulated firms and PSPs (which follow an 'initial', 'intermediate' and 'final' phase structure). Duplicative incident reporting requirements for PSPs have been removed.

Interestingly, firms who are also in scope of the EU's DORA regime will be aware that the EU is also looking to introduce a single incident reporting platform as part of its Digital Omnibus simplification package – albeit that its focus is on digital, rather than financial, legislation (the General Data Protection Regulation, NIS2 Directive, DORA, etc.).[3]

When does the obligation to report an operational incident arise?

The UK's new incident reporting regime is rooted in a common definition of 'operational incident' for the FCA, PRA and the Bank. An 'operational incident' for these purposes is defined as either a single event or a series of linked events which disrupts the firm's operations such that it:

1. disrupts the delivery of a service to an end user external to the firm; or
2. impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to such an end user.

The requirement to submit an incident report applies to operational incidents that meet one or both of these criteria, *and* meet one or more of the relevant regulator's thresholds. A potential or uncrystallised event would be considered a near-miss, and fall outside the scope of reporting.

The reporting thresholds themselves differ for each regulator, reflecting their statutory objectives. For the FCA, for example, the threshold for reporting is met where a firm reasonably believes that an operational incident meets one or more of the following notification thresholds, namely that it poses a risk:

- of causing intolerable levels of harm to consumers from which consumers cannot easily recover;
- to the safety and soundness of the firm and/or other market participants; or
- to market stability, market integrity or confidence in the UK financial system.

The PRA's thresholds are, meanwhile, focused on risks to the stability of the UK's financial system, the firm's safety and soundness, and (for insurers) protection of policyholders. Fintechs should note that PSPs have additional sector-specific factors to consider when assessing the FCA's thresholds,

because incidents in this sector are considered especially time sensitive given the fast and direct impact on consumers.

Notably, an 'end user' for these purposes is interpreted widely and could be a retail customer, business customer, other legal entity, trustee, market participant, supervisory regulator or even a member of the firm's group. The regulators further explain that a 'series of linked events' include those whose cumulative impact result in a disruption, and could include an event having cascading effects or multiple events originating from the same root cause.

Timings

Firms are required to submit an initial report as soon as reasonably practicable, and the regulators expect this to be within 24 hours of the firm determining an operational incident has met the threshold. This is with the exception of PSPs, which should continue to report incidents within four hours of detection, in line with their previous reporting regime.

Enhanced reporting firms must provide a final update within 30 working days of an operational incident being resolved unless there are exceptional circumstances. Even in such cases, the firm must submit the final phase as soon as practicable but not more than 60 working days after resolving the incident.

Bringing this together, it is clear that the new incident reporting regime will generate a significant amount of data for supervisory purposes – despite a reduction to the volume of information to be reported since the consultation proposals. Reporting on data loss incidents may prove to be the biggest step up for firms, given that that respondents to the FCA's consultation requested a higher reporting threshold specific to data loss incidents (which the FCA could not see a justification for).

Material Third-Party Reporting

The regulators have expanded the scope of existing outsourcing notifications to create a unified FCA, PRA and Bank reporting regime for both material outsourcing and non-outsourcing arrangements under the banner of 'material third-party arrangements'. Examples of non-outsourcing third-party arrangements for these purposes may include buying or acquiring hardware, software and other ICT products, such as designing and building an on-premise IT platform, or advanced analytics models developed by third parties.

A standard process for notifying the regulators of new material third-party arrangements, and of significant changes to existing ones, has been introduced, using a single template on a single portal, so firms make one submission regardless of which regulator(s) a report is for.

Firms will additionally be required to maintain a register of their material third-party arrangements in a standardised format, and submit it annually. Together, these requirements seek to aid better identification of the risks posed by third-party service providers, and support the recommendation of certain CTPs to be designated by HM Treasury under the new CTP regime.

The requirements apply to enhanced scope Senior Managers and Certification Regime firms, dual-regulated firms, CASS large firms, UK RIEs, authorised e-money and payment institutions and consolidated tape providers. Notably, while third-country branches of international firms are excluded from the notification requirements, they are in scope of the requirement to submit an annual material third-party register.

When does the obligation to report a material third-party arrangement arise?

As described above, in-scope firms must notify the regulators of new material third-party arrangements and significant changes to existing ones. A 'third-party arrangement' is defined broadly as an arrangement of any form between a firm and a person who provides a product or service to the firm, whether or not the product or service is:

a) one which would otherwise be provided by the firm itself;
b) provided directly or by a sub-contractor; or
c) provided by a person within the same group as the firm.[4]

The regulators then have different approaches to defining '*material* third-party arrangement' based on their statutory objectives. The FCA definition is a third-party arrangement which is of such importance that a disruption or failure in the performance of the product or service provided to the firm could:

a) cause intolerable levels of harm to the firm's clients;
b) pose a risk to the soundness, stability, resilience, confidence or integrity of the UK financial system; or
c) cast serious doubt on the firm's ability to satisfy the threshold conditions, or meet its obligations under the Principles, or under SYSC 15A (Operational resilience).

The PRA's definition, meanwhile, focuses on the stability of the UK's financial system, the firm's safety and soundness, and (for insurers) protection of policyholders. The PRA and FCA provide examples of third-party arrangements that are normally material, and in both cases, these include services for storing sensitive information, such as data centres or cloud services, and using AI models for trading.

Timings

The notification requirement arises when a material third-party arrangement is planned or there is a significant change to the arrangement. A 'significant change' for these purposes is a change that materially alters the nature, scale or complexity of the risks inherent to the arrangement. This could include a change in how the third party stores, processes or accesses sensitive data, moving data storage to a new location, or a change in a key sub-contractor. There are no prescribed timelines for submitting or reviewing notifications. However, firms are expected to notify at an early stage and to submit the notice before making any internal or external commitments.

For the material third-party register, firms are not expected to resubmit the register each time a notification is required. Regulators will notify relevant firms of their register reporting requirements when the annual submission window opens, and these firms will have 90 calendar days to make their submission using the template provided.

Next Steps and Reflections

The new rules and guidance will come into force on 18 March 2027, giving firms 12 months to prepare for compliance. There is plenty to do here for individual firms over the next year, including work to map the new rules against existing incident notification requirements, to establish which arrangements qualify as a material third-party arrangement, and to ensure contracts with third parties support the requirement to report a 'significant change' to a material third-party arrangement.

For those with an EU nexus, the requirements are intended to be broadly aligned with those under the EU's DORA, but they are not replicated exactly. These firms will therefore need to get to grips with new UK rules and adapt their processes to manage the differences between the EU and UK regimes.

Firms will also need to understand how these new requirements complement (and extend beyond) the existing framework for operational resilience. Notably, an incident can meet the definition of an 'operational incident' regardless of whether it impacted the delivery of an 'important business service' under the current operational resilience framework. Similarly, notification of material third-party arrangements is not limited to those third-party arrangements affecting an important business service.

Taking a broader view, the impact of operational incident and material third-party data reporting on supervisory strategy is likely to be significant in the medium to long term. These requirements will take hold at a pivotal moment of convergence between financial services and technology, where traditional financial services are increasingly delivered via digital platforms and apps, and technology firms are offering payment wallets and credit options. It is also a time of unprecedented innovation as AI and blockchain, in particular, drive new products, services and payment rails. As the financial sector evolves at rapid pace, the regulators have armed themselves with the data to keep up.

Endnotes

1 FCA Policy Statement PS26/2: Operational incident and third party reporting (18 March 2026). Available at: https://www.fca.org.uk/publications/policy-statements/ps26-2-operational-incident-third-party-reporting

PRA Policy Statement PS7/26: Operational resilience – Operational incident and third-party reporting (18 March 2026). Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2026/march/operational-incident-and-third-party-reporting-policy-statement

Bank of England Policy Statement: Operational resilience – Operational incident and third-party reporting for FMIs (18 March 2026). Available at: https://www.bankofengland.co.uk/paper/2026/ps/operational-resilience-operational-incident-and-outsourcing-and-third-party-reporting-for-fmis

2 David Shone, Martijn Stolze, Tabitha Harris & Emily Bradley, 'EU and UK Operational Resilience: One Aim, Two Approaches', in David Ives, David Shone & James Cook (ed.) *ICLG – Fintech 2025*, Global Legal Group, pp 1–3.

3 Slaughter and May: EU proposes single-entry point for cyber incident reporting, but is it really "report once, share many"? (11 December 2025). Available at: https://thelens.slaughterandmay.com/post/102lxgd/eu-proposes-single-entry-point-for-cyber-incident-reporting-but-is-it-really-re

4 While firms should not treat an intragroup arrangement as being automatically less risky when assessing its materiality, it is worth flagging that most firms are only required to report intragroup arrangements where an external third-party dependency exists, in order to reduce the reporting burden.

David Shone is co-head of our Fintech group, and advises fintechs, traditional financial institutions and investors on commercial and regulatory issues of strategic importance to their businesses, including fundraising, governance, capital structuring, outsourcing arrangements and product development. His clients include Monzo, Tencent, Teya, Credit Karma and TreasurySpring alongside traditional financial institutions such as Barclays, Nationwide, Santander, Aviva and Standard Chartered.

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom

Tel: +44 20 7600 1200
Email: david.shone@slaughterandmay.com
LinkedIn: www.linkedin.com/in/david-shone-a21b43121

Natalie Donovan is head of knowledge in our Tech & Digital group, with a particular emphasis on strategic sourcing, cyber and digital regulation. She helps clients with their cyber preparedness activities and regularly writes and speaks on cyber, outsourcing, AI and other technology issues.

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom

Tel: +44 20 7600 1200
Email: natalie.donovan@slaughterandmay.com
LinkedIn: www.linkedin.com/in/natalie-donovan-869b6b82

Emily Bradley is knowledge counsel in our Financial Regulation group, with a particular emphasis on fintech. She originates thought leadership for both clients and academic publishers, and is actively involved in industry groups focused on the role of emerging technologies in financial services.

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom

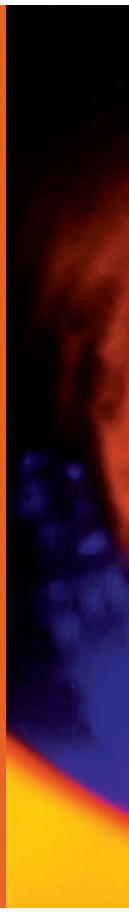
Tel: +44 20 7600 1200
Email: emily.bradley@slaughterandmay.com
LinkedIn: www.linkedin.com/in/emily-bradley-100125255

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Fintech 2026 features one expert analysis chapter and 29 Q&A jurisdiction chapters covering key issues, including:

- The Fintech Landscape
- Funding For Fintech
- Fintech Regulation
- Other Regulatory Regimes / Non-Financial Regulation
- Technology



The International Comparative Legal Guides are published by: glg Global Legal Group