



AFB Seminar: Navigating the Operation of Financial Crime Controls

30 September 2026



Association of Foreign Banks (AFB) foreignbanks.org.uk



Pinsent Masons

A purpose-led professional services business
with law at the core

Navigating the Operation of Financial Crime Controls

Melanie Ryan
30 September 2026

Agenda

- Key legislation, regulations and guidance underpinning the financial crime regime in the UK
- Main money laundering offences for banks
- SAR regime
 - Issues and recent changes
 - Practical considerations
 - Customer challenge
- Section 333A of POCA – "Tipping Off"
 - *R v Osmond [2026] EWCA Crim 979*
 - Corporate criminal liability
- Case study – reporting obligations and possible offences
- FCA approach to financial crime and enforcement activity
- Cooperation and data sharing between authorities – current and future

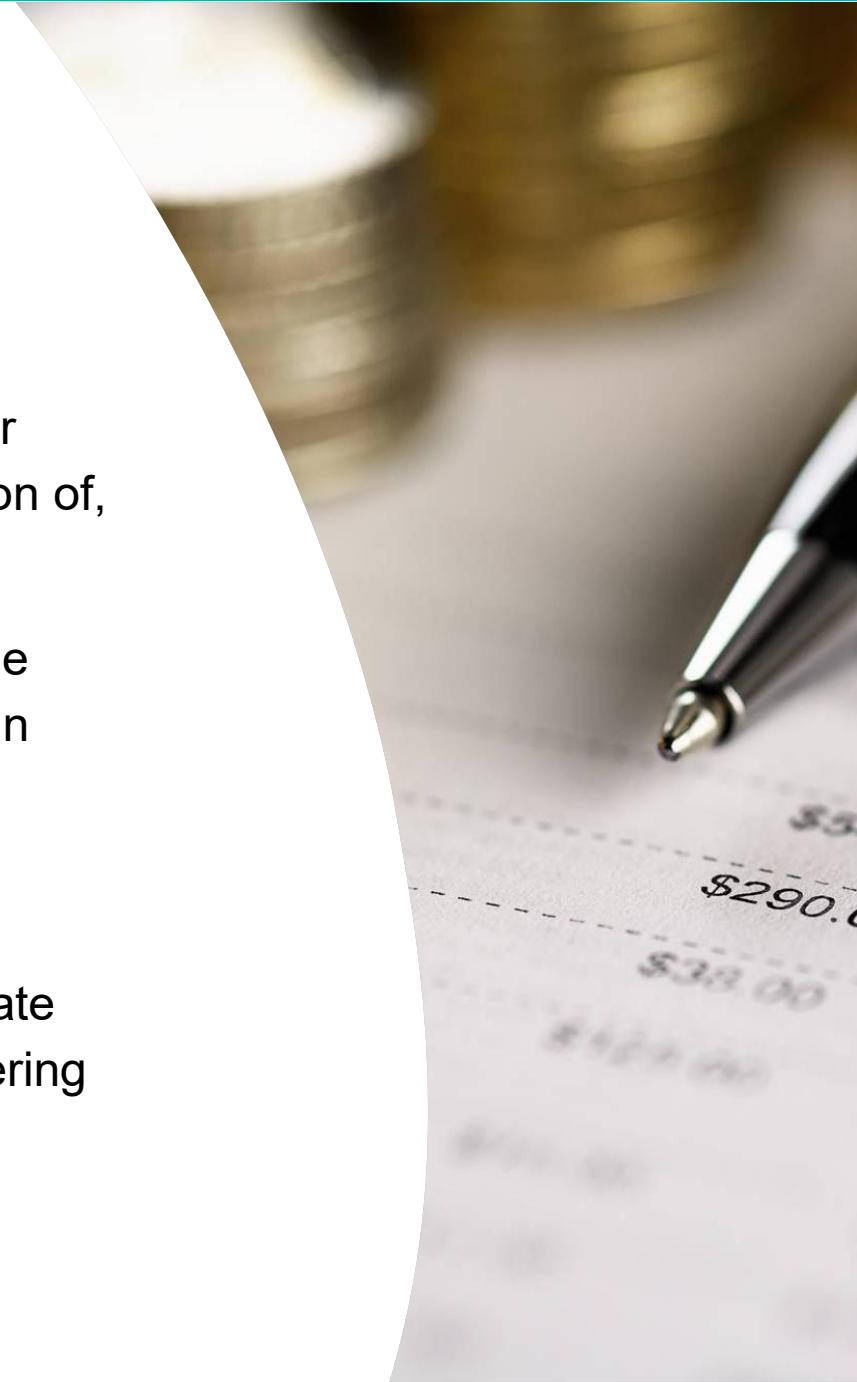
Financial crime in the UK – Key legislation, regulations and guidance for banks

- Proceeds of Crime Act 2002 (as amended) (POCA)
- Terrorism Act 2000 (as amended) (TACT)
- Criminal Finances Act 2017
- Sanctions and Anti-Money Laundering Act 2018 (SAMLA)
- Economic Crime and Corporate Transparency Act 2023 (ECCTA)
- Crime and Policing Act 2026
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (MLR 2017)
- FCA Handbook: SYSC
- FCA Financial Crime Guide (FCG)
- Joint Money Laundering Steering Group (JMLSG) Guidance

Main money laundering offences for banks

POCA and MLR

- Three broad groups of offences:
 - Knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property
 - Failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering
 - Tipping off or prejudicing an investigation
- In addition, under the MLR, it is a separate offence not to establish adequate and appropriate procedures in place to counter and prevent money laundering



SAR Regime

Issues / shortcomings

- Low statutory thresholds have led banks to file large volumes of frequently low-quality suspicious activity reports (SARs) in order to avoid non-compliance
 - 2024-2025 UKFIU received 866,616 SARs, over 85% of which was from the financial services industry (just under 79% from banks alone)
- Test for 'suspicion' is low
 - Threshold defined by case law as a 'possibility, more than fanciful, that the relevant facts exist' *R v Da Silva* [2006]
- Drain on internal banking resources without generating actionable intelligence
 - Data moves from banks to law enforcement with very little feedback or reciprocity allowing banks to improve their own risk profiles

SAR Regime

Issues / shortcomings

- Under-utilisation by law enforcement of massive quantities of data received
 - Defence Against Money Laundering (DAML) SARs successfully freeze millions but make up a tiny fraction of the system output
 - Record-high £382.6 million was denied to suspected criminals via DAML requests in 2024-2025, representing a 59% increase in value
- Focus is on single transactions
 - Static controls mean that there is a failure to flag massive and sophisticated interconnected money laundering such as 'money mule hubs'

SAR Regime

Recent changes

- Amendments to POCA (introduced by ECCTA (s183))
 - Sections 327(2F), 328(8), and 329(2F) of POCA came into effect in January 2024
 - Provide exemptions for mixed-property transactions
 - Allow a bank to manage accounts containing both legitimate and ring-fenced criminal funds without needing a DAML for everyday operations, provided the remaining funds do not dip into the ring-fenced amount.
 - A SAR detailing the 'ring fenced' amount still has to be filed.
 - Should further suspicion arise, or the 'ring fenced' funds need to be accessed for whatever reason, then a DAML will be needed.

SAR Regime

Recent changes

- Threshold amount under s339A of POCA – which was £1,000 and is now (since end July 2025) £3,000 - under which an account can:
 - (i) continue to be operated; or
 - (ii) be closed and funds 'paid away'without seeking a DAML from UKFIU, even if criminal property is suspected
- Is the threshold amount still too low or does it increase "smurfing" risk?

Practical considerations following SAR filing

- Generally accepted rule of thumb: you can communicate the action being taken – the "what" – but not the reason – the "why"
- Use standard, objective and neutral scripts which mirror ordinary commercial or operational procedures
 - For example:
 - The transaction is currently undergoing a routine review as part of our ongoing commitment to account security ...
 - As part of our regulatory obligations, we routinely review the information we hold on all customer accounts. To ensure our records remain accurate, would you please provide ...
 - Following a recent review, we have made commercial business decision to close your accounts with immediate effect. This decision has been made in accordance with paragraph [...] of our standard terms and conditions.
 - The scripts should be strictly adhered to.

Practical considerations following SAR filing

- Route all escalations through a single channel controlled by the nominated officer / MLRO.
 - Complaints should be handled by the fin crime team, not the general complaints team.
- Ensure centralised control and restrict access to information
 - The SAR log should not be accessible by frontline or support staff.
- Dual-track logging (in order to comply with POCA, MLRs and FCA expectations)
 - The restricted SAR log, accessible by MLRO / nominated officer team which should record:
 - The internal trigger and initial suspicion
 - The MLRO's investigation and analysis
 - The decision to file / not to file a SAR and why
 - Tipping off control record
 - Client file / CRM trail
 - Objective event / action taken
 - Communication transmitted

SARS – Customer challenge

- Customers frequently complain when their accounts are frozen or a specific transaction is blocked.
 - Complaints are exacerbated by the bank's inability to provide an explanation which the customer finds acceptable
- Complaints to FOS
 - Approximately 33,000 complaints to FOS relate to current accounts of which approximately 4,000 relate to 'debanking' (sudden terminations without notice) and 10,000 relate to account freezes and blocks (generally driven by algorithmic AML triggers)
 - FOS rules in favour of the consumer in roughly 25% - 36% of disputed account closure cases, depending on the year
 - Successful challengers will receive compensation and an apology; not a reopened account.

SARS – Customer challenge

- The FOS will work with the bank when a SAR has been filed (see Ch. 6 JMLSG), but will still find in favour of the consumer if the bank has not acted expeditiously and/or done what it could do within the confines of POCA
 - Metro Bank (DRN-8531177)
 - HSBC (DRN-4661098)
- Case law
 - Generally speaking, the courts will uphold banks' decisions to freeze and/or close a customer's account without notice in circumstances where they suspect money laundering or criminal activity
 - *Shah & Anor v HSBC Private Bank (UK) Ltd* [2012] EWHC 1283 (QB)
 - *N v The Royal Bank of Scotland Plc* [2019] EWHC 1770 (Comm)
 - *Harvey v Santander UK Plc* [2023] EWHC 2947 (KB)

Section 333A of POCA – "Tipping Off"

R v Osmond [2026] EWCA Crim 979

- Court of Appeal, handed down on 28 July 2026
- First appellate consideration of s333A(3) of POCA
- Section 333A(3) provides that *"a person commits an offence if—*
 - a) the person discloses that an investigation into allegations that an offence under this Part has been committed is being contemplated or is being carried out;*
 - b) the disclosure is likely to prejudice that investigation; and*
 - c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector."*



Section 333A of POCA – *R v Osmond* [2026] EWCA Crim 979

Facts

- Mr Osmond, a solicitor and senior partner of Osmond & Osmond Solicitors, acted for a long-standing client, James Ramsay, in connection with a 2013 transaction in which Mr Ramsay lent £4 million towards the purchase of an £8 million residential property in Mayfair. The loan was routed through an offshore vehicle the incorporation of which along with the loan documentation was handled by Mr Osmond. The loan monies passed through the Osmond & Osmond client account.
- The loan and the transaction came to the attention of the SFO in the context of the long-running and well-publicised investigation into ENRC. It transpired that the borrower of the £4 million and the purchaser of the Mayfair property was the wife of a senior ENRC official and daughter of one of ENRC's founders.

Section 333A of POCA – *R v Osmond* [2026] EWCA Crim 979

Facts (continued)

- On 7 June 2018, an SFO investigator called Mr Osmond about the transaction. The investigator explained that the SFO has suspicions about the £4 million which had passed through his firm's client account, including whether it constituted money laundering. The investigator also told Mr Osmond that the SFO would be requiring him to answer questions and provide documents about the transaction.
- On 15 June 2018, the SFO served a section 2 notice (under the CJA 1987) on Mr Osmond. The cover letter required Mr Osmond to keep the matter confidential and expressly made reference to the tipping off offence.
- However, on 8 June 2018, Mr Osmond had already spoken to Mr Ramsay about the SFO's inquiries and had also visited him at his home in Malta a few days later.
- Mr Osmond was prosecuted and convicted to nine months' imprisonment, suspended for 18 months.

Section 333A of POCA – *R v Osmond* *[2026] EWCA Crim 979*

On appeal:

- Mr Osmond submitted that:
 - the ENRC investigation was already public knowledge and was known to Mr Ramsay, so nothing capable of amounting to a "disclosure" within the meaning of s333A(3) had occurred.
 - the information Mr Osmond passed on had come to him from the SFO itself, in his capacity as a solicitor responding to a statutory notice, rather than in the course of a regulated business.
 - the disclosure had not caused the SFO's investigation to suffer any prejudice. The information and documents provided to the SFO were not any different as a result of any disclosure to Mr Ramsay than if Mr Osmond had provided them without Mr Ramsay's input.



Section 333A of POCA – *R v Osmond* [2026] EWCA Crim 979

- The Court of Appeal, in refusing leave to appeal, concluded:
 - On the question of disclosure, the court held that an investigation can be the subject of a disclosure under section 333A(3) even where it forms a strand or an aspect of a wider investigation whose existence is public knowledge. The prosecution's case was confined to the SFO's inquiry into the Mayfair transaction specifically which was not publicly known and nor was it known to Mr Ramsay.
 - On whether the information had been received in the course of business in the regulated sector, the court held that it was irrelevant that Mr Osmond received the information from the SFO; what mattered is not the source of the information but rather the capacity in which it is received. Mr Osmond was clearly conducting business in the regulated sector, having acted for Mr Ramsay in a property transaction involving the acquisition of an offshore vehicle and the handling of client money (Schedule 9 of POCA).

Section 333A of POCA – *R v Osmond* [2026] EWCA Crim 979

- The Court of Appeal, in refusing leave to appeal, concluded (continued):
 - On prejudice, the court held that the prosecution need only establish that a disclosure was 'likely' to prejudice an investigation at the time it was made. There is no requirement to prove actual prejudice with hindsight, and it is no defence that no prejudice in fact resulted. The court went further stating that the disclosure of the investigation is inherently likely to prejudice the investigation because of the risk that evidence will be destroyed or compromised.
- **Takeaways:**
 - A specific line of inquiry in a wider publicly known investigation constitutes an investigation in its own right for the purposes of s333A(3)
 - Assume that prejudice is likely if a disclosure is made
 - Escalation?

Section 333A(3) and Corporate Criminal Liability

- **Other considerations: Corporate criminal liability**
 - Economic Crime and Corporate Transparency Act 2023, s196 and Schedule 12
 - Schedule 12 listed economic crimes in scope of the offence and specifically included s333A
 - Crime and Policing Act 2026, section 250
 - Repealed and replaced s196 and Schedule 12 of ECCTA, expanding it to include all criminal offences
 - All corporate bodies may be held criminally liable where a "senior manager" commits any type of crime while acting within the actual or apparent scope of their authority
 - A 'senior manager' is someone who plays a significant role in making management decisions about all or a substantial part of the organisation's activities, or in actually managing or organising those activities or a substantial part of them.
 - The Notes to section 250(3) suggest that this covers both those in the chain of management as well as those in, for example, strategic compliance roles.

Section 333A and Corporate Criminal Liability

- Other considerations: Corporate criminal liability (continued)
 - Applied to *R v Osmond*: had the facts in this case occurred after 26 December 2023, Osmond & Osmond Solicitors would also have been guilty of the offence of tipping off: Mr Osmond was clearly a 'senior manager' who, in disclosing the investigation to Mr Ramsay, was acting within his actual or apparent authority.



Case study – reporting obligations and possible offences

Facts

- UK bank had two customers with business banking accounts. One customer was a small law firm and the other was a legal consultant. The consultant provided certain legal services to the law firm.
- For a period of approximately two years starting in mid-2022, several million pounds passed through the two business banking accounts, funds being generally received in the account of the consultant before being transferred to the law firm's account.
 - Not infrequently, funds were then transferred back to the consultant's account.
- In late summer 2024, the transfers between the two accounts flagged on the bank's transaction monitoring alerts. The pattern of transfers suggested that the consultant was fronting for the law firm.

Case study – reporting obligations and possible offences

Facts (continued)

- On investigation, it was found that significant sums had been received into the consultant's account which had originated (frequently indirectly) from a Russian entity which appeared to be owned and/or controlled by two designated persons.
- The funds had been transferred for the purpose of funding litigation of Russian clients of the law firm; the consultant was assisting the law firm with that litigation.
- The funds had been used to pay the law firm's fees and the consultant's fees. Funds had also been paid into court.
- The bank immediately froze both accounts and notified OFSI.
 - The last transaction originating from the Russian entity predated the freezing by about four months.

Case study – reporting obligations and possible offences

Legal issues

- *The dispute*

- The law firm and the consultant threatened to sue the bank, maintaining that the Russian entity that was the original transferor was, at the time of the first transfer back in 2022, no longer owned or controlled by designated persons.
 - There had purportedly been an arm's length transaction pursuant to which the entity it had been sold seemingly just after the owners / sellers had been designated by the UK; they had already been designated a few days previously by the EU.
 - The bona fides of the transaction was disputed by the bank.

Case study – reporting obligations and possible offences

Legal issues

- *The dispute (continued)*
 - The law firm and consultant argued in their letter before action that even if the original transferor was owned or controlled by a designated person, the funds, on their deposit on the business banking accounts, could no longer be said to be owned or controlled by a designated person as legal title had passed to the consultant / law firm.
 - In other words, by failing to intercept the funds on transfer, the bank had allowed the funds to be transferred to the consultant / law firm and for legal title to pass.
 - This was correct but only to the extent that the original transferor did not have any residual legal or equitable interest in the funds after their transfer (e.g., if the funds had been loaned for the purpose of the litigation etc.).

Case study – reporting obligations and possible offences

Legal issues

- *The dispute (continued)*
 - Interestingly, the law firm and the consultant complained to the FOS, but the FOS did not uphold their complaint; it was found that the bank had acted reasonably in freezing the accounts as it had done.
 - A forensic accounting exercise was undertaken to seek to establish whether any of the transferred funds remained in the accounts at the time they were frozen. In the case of the law firm, the bank was able to get comfortable that the funds had been fully dissipated. The same was not found for the consultant's account.

Case study – reporting obligations and possible offences

Legal issues

- *POCA*
 - At the time of freezing the accounts and notifying OFSI or shortly after, the bank also filed a SAR with the NCA.
 - Sanctions evasion is a criminal offence. The removal of the designated UBOs from the structure of the transferee constituted sanctions evasion and the funds subsequently transferred constituted criminal property.
 - The restructuring involved Luxembourg, the Netherlands and Russia
 - s330(7)(b)(i) of POCA – i.e., 'not unlawful under the criminal law applying in that country' partially engaged?

Case study – reporting obligations and possible offences

Legal issues

- *POCA (continued)*
 - Should the bank have filed a SAR at the time of the transfers? The bank didn't have any actual 'knowledge or suspicion' at the time of the transfers but arguably should have and would have had the bank's transaction monitoring and sanctions screening been more effective.
 - An offence is committed if a person '*... has reasonable grounds for knowing or suspecting that another person is engaged in money laundering*' (s330(2)(b) of POCA) and doesn't make the required disclosure (s330(4)).
 - The 'objective negligence' test
 - A person working for the bank can commit an offence despite not personally knowing of suspecting any wrongdoing, but because they were negligent in not reasonably suspecting money laundering.
 - The 'reasonable' suspicion element makes this offence different from the substantive money laundering offences where actual suspicion is required.

Case study – reporting obligations and possible offences

Legal issues

- *POCA (continued)*
 - Did the bank commit an offence under s327 of POCA by failing to block the transfers, allowing them to be deposited on the consultant's and law firm's accounts from where they were transferred to third parties and dissipated?
 - No, the bank would have had to have had subjective knowledge or a genuine suspicion that the funds were criminal property at the time of the transfers in order to commit a substantive money laundering offence.

Case study – reporting obligations and possible offences

Regulatory issues

- The issue was reported to the FCA as part of routine regulatory reporting (on RegData). No PRIN 11 notification was made.
 - Principle 11, SUP 15.3.8G(2) and FCG 7 provide that firms must consider whether they need to notify the FCA – for example, whether potential breaches of sanctions resulted from a significant failure in their systems and controls.
 - Query whether given the length of time over which the breaches occurred, how the issue was ultimately identified, the sums involved and the failure to file a SAR at the time of the transfers, it should have been subject to a PRIN 11 notification.

FCA approach to financial crime

- Fighting financial crime one of the FCA's four pillars / priorities in its strategy for 2025-2030
- Current move to a more assertive, data-driven and intervention-led approach to supervising financial crime and a corresponding move away from long retrospective enforcement action
 - Increased use of s166 reviews and VREQs
- However, at the same time, there is an arguable move back to lighter touch regulation
 - FCA has indicated that it expects industry to 'do the right thing' and those which are seen to be doing so will be treated accordingly.
 - Part of government push to drive growth

FCA Enforcement Activity

- As at 2025/2026 – over 75% of enforcement work focuses on financial crime. This includes fraud and scams, organised crime, weaknesses in AML systems and controls, and market abuse.
 - Of the 75%, 56% is fraud and scams and the remaining 18% is systems and controls.
- Between 2021-2025, there were 13 cases where the FCA took enforcement action for money laundering breaches.
 - These 13 cases generated more than £608 million in penalties which is more than half (54%) of the total amount of penalties for all enforcement action over the same period.
 - Figures are skewed by the NatWest criminal prosecution in 2021 but still demonstrates the gravity with which AML failings are treated by the FCA.
 - NatWest – Penalty: £264 million; first criminal prosecution under the MLRs
 - In the cohort, there was a mix of large high street banks, foreign-owned banks and challenger banks.

FCA Enforcement Activity

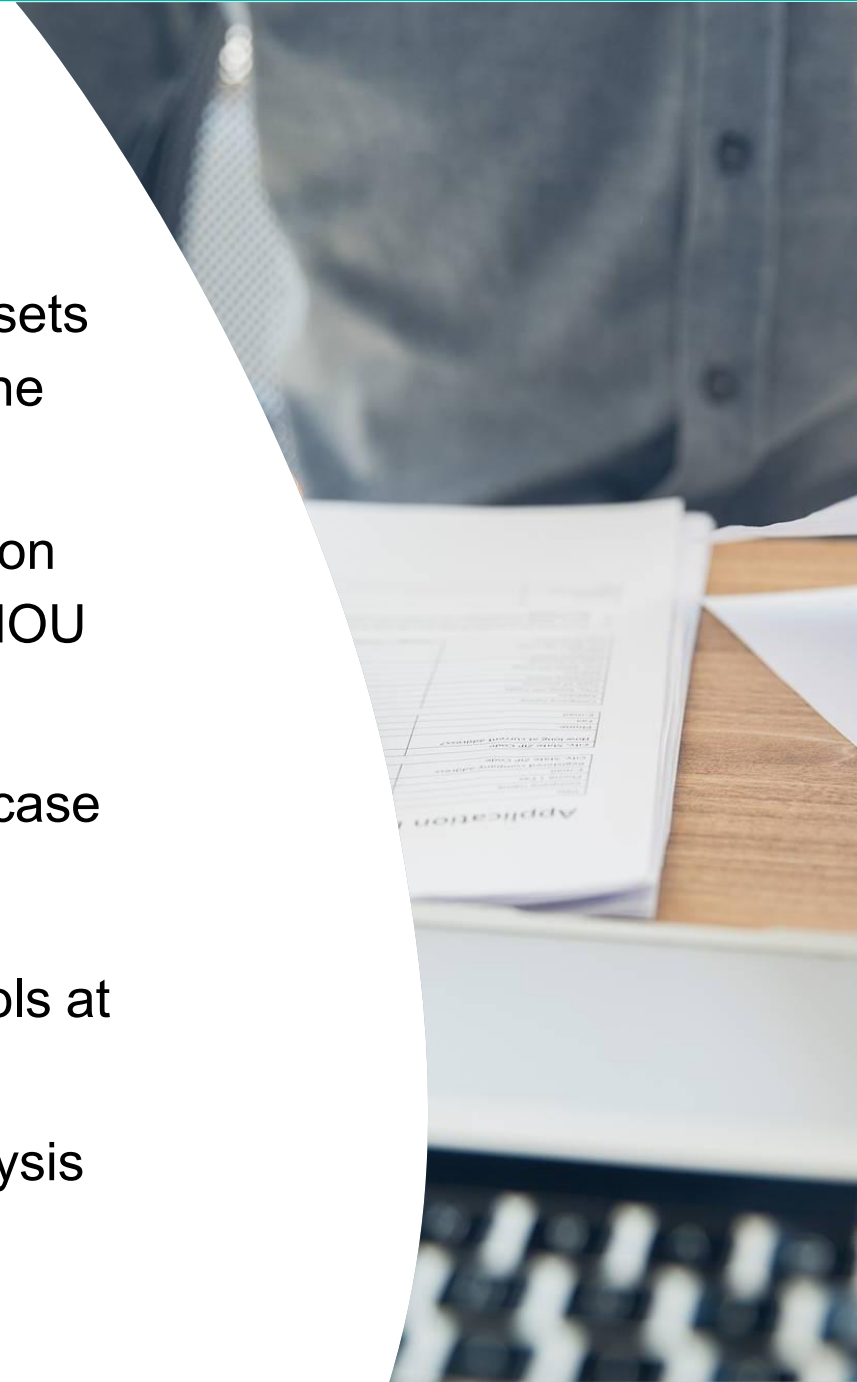
- Analysis of the 13 AML cases shows an interesting trend:
 - The earliest four cases whose findings were published between December 2021 and October 2022 all involved breaches of the Money Laundering Regulations 2007.
 - Regulations 14 (EDD) and 20 (systems and controls) of MLR 2007 most common breaches.
 - The subsequent nine cases, published between December 2022 and December 2025, all involved breaches of the FCA Handbook.
 - Principle for Business 3 (management and control) and SYSC 6.1R (adequate policies and procedures to counter financial crime) were the most common breaches.
 - Several of the nine cases reference the MLRs 2007 / 2017 but as underlying evidence of requirements, not actual breaches.

FCA Enforcement Activity

- These cases suggest a shift away from direct enforcement of specific or technical MLR breaches towards broader Principle 3 and SYCS system and control failings, enabling the FCA to challenge and take action in respect of governance, oversight, onboarding, monitoring and remediation weaknesses across entire AML – and financial crime – frameworks
 - e.g., Starling Bank (AML & sanctions failings)
- Evolution of enforcement strategy rather than a change in the underlying misconduct
 - Allows greater flexibility and arguably lowers the evidential burden
 - Average fine in the Rulebook group (larger, excluding NatWest) supports this
- For the foreign banks, EDD failings are a recurrent theme across both the 'MLR' and 'Handbook' groups.
 - Arguably reflective of the higher risk jurisdictions in which business is conducted.

Cooperation and data sharing between authorities – current and future

- Data sharing is focused on intelligence and analytics of large data sets to identify emerging risks. This includes SAR analyses shared by the NCA with the FCA.
 - In our case study, there was no evidence of any communication between OFSI and the FCA (although events pre-dated the MOU signed earlier this year) or OFSI and the NCA.
 - Contact would not necessarily be expected on a case-by-case basis, although this may change.
 - In 2022, the FCA published its review of financial crime controls at challenger banks
 - Findings of the review were in part informed by trend analysis undertaken by the UKFIU



Cooperation and data sharing between authorities – current and future

- The UKFIU found a substantial increase in the volume of SARs and DAML requests from challenger banks as they exit customers for financial crime reasons.
 - For the FCA, this raised concerns about the adequacy of the banks' CDD and EDD checks at onboarding. Also had concerns about the quality of SARs.
- Anti-Money Laundering and Asset Recovery Strategy 2026-2029 (AMLAR), published 15 September 2026
 - Establishment of National Financial Intelligence Service (NFIS)
 - Objectives: target, integrate, empower
 - Strengthen the UKFIU
 - Proposal to move the legal test under POCA from low 'suspicion' to 'reasonable grounds to suspect'
- FATF evaluation of UK – June 2027

Speaker



Melanie Ryan

Partner

+44 20 7667 0241

+44 7951 313 557

@melanie.ryan@pinsentmasons.com

Melanie specialises in commercial litigation and disputes, corporate and regulatory investigations, and related enforcement proceedings. Her areas of expertise include financial crime, bribery and corruption, money-laundering, fraud, tax and UK and EU sanctions.

Her experience includes advising and acting for financial services in complex disputes as well as internal and government investigations, frequently across multiple jurisdictions. She has extensive experience of dealing with regulators including the Financial Conduct Authority, the Prudential Regulation Authority and the Serious Fraud Office in the UK and the Department of Justice and the Securities and Exchange Commission in the US, as well as regulators and government bodies in various other jurisdictions around the world.

Melanie undertakes complex high value high court litigation and has a particular expertise in capital markets disputes including derivatives and securitisation cases. Her financial services experience includes acting for regulated entities in Enforcement investigations and proceedings, conducting shadow s166 reviews as well as advising clients on contentious regulatory matters such as Principle 11 issues and large remediation programmes.

Melanie is in the "Hall of Fame" for Banking Litigation (Investment & Retail) and is a "Leading Partner" for Financial Services - Contentious in the Legal 500.



Our Financial Services - Contentious Team



Melanie Ryan

Partner

☎ +44 20 7667 0241

📱 +44 7951 313 557

@ melanie.ryan@pinsentmasons.com



Joanne Gillies

Partner

☎ +44 141 567 8638

📱 +44 7785 720 605

@ joanne.gillies@pinsentmasons.com



Stuart Murdoch

Partner

☎ +44 131 225 0160

📱 +44 7483 711 791

@ stuart.murdoch@pinsentmasons.com



Jessica Wicker

Partner

☎ +44 20 7054 2743

📱 +44 7388 383 459

@ jessica.wicker@pinsentmasons.com



Jonathan Cavill

Partner

☎ +44 20 7418 7014

📱 +44 7775 546 063

@ jonathan.cavill@pinsentmasons.com



Ian Stott

Partner

☎ +44 113 294 5273

📱 +44 7483 113 343

@ ian.stott@pinsentmasons.com



Stuart McNeill

Partner

☎ +44 20 7054 2624

📱 +44 7969 825 452

@ stuart.mcneill@pinsentmasons.com



Jennifer Craven

Partner

☎ +44 20 7054 2596

📱 +44 7545 426 770

@ jennifer.craven@pinsentmasons.com



Mike Hawthorne

Partner

☎ +44 20 7667 0150

📱 +44 7554 222 654

@ mike.hawthorne@pinsentmasons.com

OUR GLOBAL REACH

With 31 offices across four continents,

we can help you meet your challenges, wherever they may be.

United Kingdom

London (Headquarters)
Aberdeen
Belfast
Birmingham
Edinburgh
Glasgow
Leeds
Manchester

Europe

Amsterdam
Dublin
Düsseldorf
Frankfurt
Luxembourg
Madrid
Munich
Paris
Warsaw

Asia Pacific

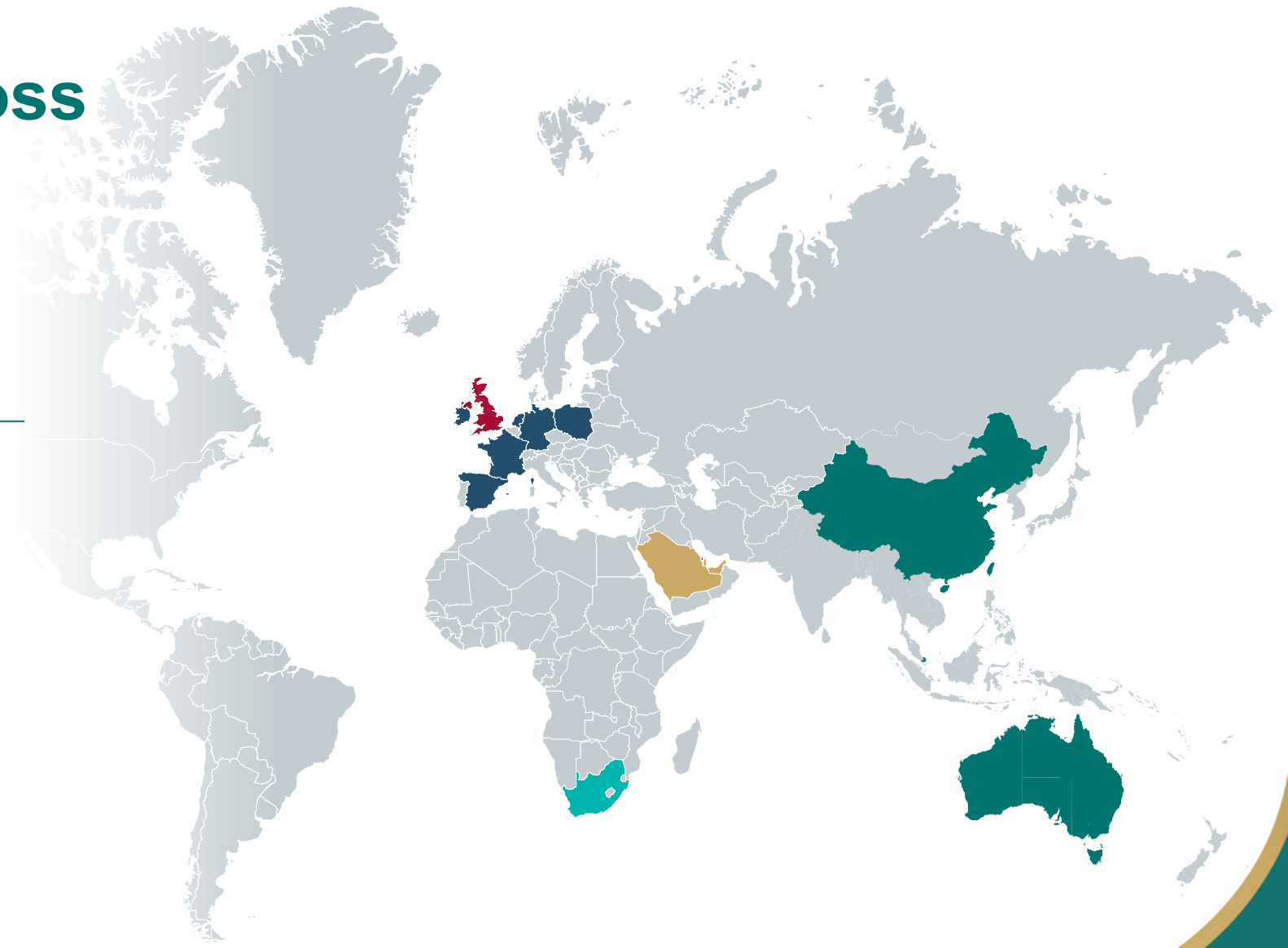
Beijing
Hong Kong
Shanghai
Shenzhen
Singapore
Melbourne
Perth
Sydney

South Africa

Cape Town (International Delivery Centre)
Johannesburg

Middle East

Abu Dhabi
Doha
Dubai
Riyadh





**Please scan QR code to
leave feedback**



Association of Foreign Banks (AFB) foreignbanks.org.uk