Practical Law™

Slaughter and May's banking and investment services column: April 2021

by Financial Regulation group, Slaughter and May

Status: **Law stated as at 27-Apr-2021** | Jurisdiction: **United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-030-7441**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

The Financial Regulation group at Slaughter and May, including partners Ben Kingsley and Nick Bonsall, and professional support lawyer Selmin Hakki, regularly share their thoughts with Practical Law Financial Services subscribers on topical developments in the banking and investment services sector.

In their column for April 2021, Ben, Nick and Selmin consider the FCA bringing criminal proceedings against National Westminster Bank plc for alleged breaches of the Money Laundering Regulations 2007, the Bank of England reminding the Chief Executive Officers of the major UK banks to prepare for the Resolvability Assessment Framework (RAF) and the PRA's March 2021 policy statements and supervisory statements on outsourcing and third party management and operational resilience.

FCA's tough stance on AML transgressions

In March 2021, National Westminster Bank plc became the first UK bank to face criminal charges for alleged breaches of the Money Laundering Regulations 2007 (MLR 2007).

Although they are no longer in force, the MLR 2007 may still be enforced for conduct occurring before 26 June 2017. To date, the FCA (and the FSA before it) had opted to impose civil, albeit sometimes weighty, fines for money laundering-related breaches, rather than pursuing criminal proceedings. Criminal proceedings raise significant issues for banks and others in the regulated community, not only for the reputational sting of any conviction, but because it will inevitably also raise concerns about the impact for senior individuals, for the firm's regulatory permissions, and the possible trigger of contractual provisions including events of default under financing and derivative arrangements.

The FCA alleges that the bank failed to satisfy regulations 8(1), 8(3) and 14(1) of the MLR 2007 which required the bank to determine, conduct and demonstrate risk-based due diligence and ongoing montoring to prevent money laundering. More specifically, and significantly, the FCA says that the bank's systems and controls failed to monitor and scrutinise increasingly large deposits into a single customer account, amounting to £365 million, much of it in cash deposits, between 2011 and 2016.

Consider the signals made by Mark Steward (Director of Enforcement and Market Oversight at the FCA) in April 2019:

> "We are now conducting "dual track" AML investigations, i.e. investigations into suspected breaches of the Money-Laundering Regulations that might give rise to either criminal or civil proceedings. I don't think there should be anything controversial here... I think it is time that we gave effect to the full intention of the Money-Laundering Regulations which provides for criminal prosecutions. In making poor AML systems and controls potentially a criminal offence, the MLRs are signalling that, in egregious circumstances, MLR failures let down the whole community and in this sense, they may constitute:
>
> "...a breach and violation of public rights and duties which affect the whole community, considered as a community; and are distinguished by the harsher appellation of crimes and misdemeanours." (Commentaries on the Laws of England (1765-69), William Blackstone.)

This does not mean every investigation where we think there is a case to answer will or should be prosecuted in this way. I suspect criminal prosecutions, as opposed to civil or regulatory action, will be exceptional. However, we need to enliven the jurisdiction if we want to ensure it is not a white elephant and that is what we intend to do where we find strong evidence of egregiously poor systems and controls and what looks like actual money-laundering."

On the facts so far disclosed, the evidence does indeed at least raise a few eyebrows, so the deployment of the FCA's criminal powers is not unexpected in light of Mr Steward's comments. Still, it may well serve to prompt some firms to (re)consider whether AML programmes still fully measure up to regulatory standards.

The FCA is obliged by FSMA to protect and enhance the integrity of the UK financial system, so this will remain a permanent area of focus. Looming in the background though are somewhat disparaging remarks made by the FATF back in 2018 that "*the UK is not yet able to demonstrate that its level of prosecutions and convictions of high-end ML is fully consistent with its threats, risk profile and national AML/CFT policies*". In finding its feet as a prosecutor, the FCA is undoubtedly also playing its role in enhancing the UK's international profile.

The risk-based approach to the monitoring and management of financial crime in the UK - as is required by the MLR 2007 and enshrined in the JMLSG guidance - means it will never be possible to detect and prevent all instances of money laundering. This was acknowledged in an exchange of letters between the FSA and the JMLSG in 2006 in which, in a letter dated April 2006, the FSA told the JMLSG:

> "... in a risk-based approach things sometimes go wrong: zero failure is not only impossible to achieve, aiming for it is the opposite of good regulation and a blueprint for fighting money laundering poorly. We recognise that some firms have concerns that if they follow a risk-based approach we might challenge their actions on the basis of hindsight and sanction them for any misjudgement. But if a firm demonstrates that it has put in place an effective system of controls that identifies and mitigates appropriately the risks that it is used for money laundering, enforcement action is very unlikely."

But the regulator will feel it needs to respond forcefully when high profile examples of poor conduct arise. While it seems unlikely that the FCA will mount a prosecution against a firm for AML failures absent "*strong evidence of egregiously poor systems and controls*" of the type that "*let down the whole community*", there is plainly no room for complacency.

How to fix a broken bank

At the end of February, Dave Ramsden (Deputy Governor for Markets and Banking at the Bank of England (BoE)) sent a letter to the Chief Executive Officers of the major UK banks to remind them to prepare for the Resolvability Assessment Framework (RAF).

The RAF is the final major piece in the UK's resolution regime puzzle and a key priority for the BoE, as the UK's resolution authority, this year. Details are set out in a PRA policy statement (PS15/19), a supervisory statement (SS4/19) (and the Resolution Assessment Part of the PRA Rulebook).

In short, the RAF is designed to make resolution "*more transparent, better understood and more successful*". It requires certain major UK banks to perform a "realistic" assessment of their preparations for resolution, including the identification of any barriers and plans to address them. Banks will need to submit a report of that assessment to the PRA by October 2021. They will also be required to publish a summary of that report by June 2022, with reference to the following three resolvability outcomes:

- Having sufficient financial resources available to absord losses and enable recpaitlaisation during resolution without exposing public funds to loss.
- Being able to continue to do business during resolution and any susequent restructuring.
- Being able to co-ordinate and communicate effectively within the firm and with the authorities and markets so that resolution and subsequent restructuring are orderly.

Banks must "*identify, design and implement the capabilities necessary to achieve these outcomes*", with due consideration of how their specific structure or business model may prevent them from being satisfied. There are several good practice examples of how this is to be achieved in the BoE's February letter, framed against each of the three outcomes.

All this should build on work that has already been done by firms to be considerd resolvable since the financial crisis. But it is perhaps the first time banks have been required "*to think holistically about their resolvability*", as this BoE article puts it.

Aside from accountability, transparency is the other key strand to the RAF. The BoE will itself issue a public statement concerning the resolvability of the relevant banks. Mr Ramsden notes:

> "Greater transparency will ... mean firms can be held to account for their progress on resolvability. Driving forward progress on resolvability is critical, and by allowing firms to demonstrate their progress through high-quality disclosures, the RAF also presents firms with a strategic opportunity to reinforce their reputation as safe and sound financial institutions. In this context, the Bank's public statement on resolvability, to be published by June 2022, will include views on individual firms."

The Bank's statement will not constitute a "pass" or "fail" judgement on each firm's resolvability "*in*

recognition that resolvability is a complex judgement", but will increase public knowledge about banks' readiness for resolution. It will also send a welcome signal to investors that another significant milestone in the implementation of post-crisis reforms has been achieved.

Outsourcing and dependency management

The PRA has published a policy statement on outsourcing and third party management (PS7/21) including the text of a supervisory statement (SS2/21) which "*clarifies, develops, and modernises*" longstanding regulatory requirements and expectations in this area. The PRA's policy statement on operational resilience (PS6/21) was published simultaneously and should be considered in conjunction with PS7/21.

The rising tide of guidelines and recommendations on outsourcing, third party risk management, cloud outsourcing and information and communication technology (ICT) risk management that has been emerging from supervisory authorities and other standard setters can be somewhat overwhelming.

SS2/21 implements the EBA outsourcing guidelines as well as parts of the EBA ICT guidelines relevant to the management of ICT third-party risk. Firms subject to SS2/21 are not expected to comply with the EIOPA cloud guidelines, the EIOPA ICT guidelines or ESMA guidelines on outsourcing to cloud service providers.

The expectations in SS2/21 "*are not materially divergent*" from the EBA outsourcing guidelines, but they do elaborate in parts where it has been deemed expedient to advance the PRA's objectives. There is, for example, some additional granularity in Chapter 7 on data security and Chapter 10 on business continuity and exit plans (to complement the PRA's policy on operational resilience and also ostensibly to apply lessons gleaned by the PRA in its supervision and enforcement experience to date).

SS2/21 also provides more detailed guidance than the EBA outsourcing guidelines on the application of proportionality to intragroup outsourcing and outsourcing arrangements for third-country branches, as requested by respondents to the underlying PRA consultation. None of this changes the fundamental premise that intragroup arrangements are not to be treated as inherently less risky than arrangements with third parties outside a firm's group, but there is scope for firms to make some practical management adjustments. In some cases, firms may rely on business continuity, contingency, and exit plans developed at the group level.

SS2/21 will apply to all forms of outsourcing and certain non-outsourcing third party arrangements entered into by firms, confirming what we have assumed for some time: that third party operational dependencies which do not quite meet the definition of an outsourcing should still be risk-managed as if they were:

> "The PRA maintains that certain non-outsourcing third party arrangements might be highly relevant to the PRA's objectives; for instance, if they support the provision of important business services. Therefore, the SS sets out the expectation that firms should assess the materiality and risks of all third-party arrangements using all relevant criteria in Chapter 5 of the SS, irrespective of whether they fall within the definition of outsourcing. Firms should attach greater importance to the dependencies and risks that their outsourcing and third-party arrangements create than to specific definitions."

There are also several PRA requirements, including the Fundamental Rules and the new requirements in the Operational Resilience Part of the PRA Rulebook, which apply to and govern the management of all third-party arrangements, irrespective of whether they fall under the definition of outsourcing (all of which are helpfully listed in SS2/21). Examples of non-outsourcing third-party arrangements might include the design and build of an on-premise IT platform, the purchase of data collated by a third party, and the purchase of "off the shelf" machine learning models.

As for the criteria in Chapter 5 of SS2/21, it is noted that a firm should generally consider an outsourcing or third-party arrangement as material where a defect or failure in its performance could materially impair:

- The financial stability of the UK.
- Firms' ability to meet the Threshold Conditions, compliance with the Fundamental Rules, requirements under "relevant legislation" and the PRA Rulebook.
- Safety and soundness.
- (For insurers only) the ability to provide an appropriate degree of protection for those who are or may become policyholders in line with the PRA's statutory objectives; and the requirement not to undermine the "continuous and satisfactory service to policyholders".
- Operational continuity in resolution (OCIR) and, if applicable, resolvability.

Generally speaking, an outsourcing arrangement will be classified as "material" if the service being outsourced involves an "*entire 'regulated activity'*" (portfolio management is provided as an example) or an "*internal control or key function*".

Even if none of these criteria apply, firms are expected to consult a list of factors in SS2/21 to further assess the materiality of a particular outsourcing or third-party arrangement.

Where a firm deems non-outsourcing third-party arrangements to be material or high risk, there should be effective, risk-based controls that:

> "... do not necessarily have to be the same as those that apply to outsourcing arrangements. However, the controls should be appropriate to the materiality and risks of the third-party arrangement and as robust as the controls that would apply to outsourcing arrangements with an equivalent level of materiality or risk. It follows that firms should apply stricter controls to material, non-outsourcing third-party arrangements than to non-material outsourcing arrangements."

SS2/21 will ultimately constitute "*the primary source of reference for UK firms when interpreting and complying with PRA requirements on outsourcing and third-party risk management.*"

Outsourcing arrangements entered into on or after 31 March 2021 should meet the expectations in SS2/21 by 31 March 2022. Legacy outsourcing agreements entered into before 31 March 2021 will need to be reviewed and updated at the first appropriate contractual renewal or revision point to meet these expectations.

For our analysis of the EBA guidelines on outsourcing, which took effect on 30 September 2019, see Article, Time to re-examine outsourcing: new EBA guidelines in force.