PAYMENT SERVICES AND E-MONEY FIRMS

October 2022

IDEAS | PEOPLE | TRUST

WELCOME TO OUR REGULATORY UPDATE FOR PAYMENT SERVICES AND E-MONEY FIRMS

I hope that you have all been able to enjoy the exceptional summer.

We are pleased to introduce BDO's first Payments and E-money Regulatory Update which summarises the key regulatory developments and emerging business risks relevant for all Payment Institutions and E-money Institutions.

Our Financial Services Internal Audit and Advisory teams consist of ex regulators, heads of Internal Audit and Advisors. We are working with a multitude of Payments and E-money firms as internal auditors and advisors, giving us a broad perspective on the issues facing the sector. We have insights from our in-house research team, the Regulators and professional bodies, including the Chartered Institute of Internal Auditors (CIIA), to support your regulatory considerations and activities.

We have seen an uptick in the regulatory oversight, requiring firms within this sector to enhance their internal processes and controls. There has been significant focus on Safeguarding and Outsourcing and with the recently published Consumer Duty the focus on firms will only continue to increase. The sector and firms are growing and have an expectation to grow rapidly within the current market resulting in resource capacity issues not just within firms but also within the market.

We have provided a selection of the key themes and areas that we hope will be of value to you and your colleagues; please do share with us any feedback you may have for our future editions and would be happy to discuss any points of interest further.

LUKE PATTERSON

Partner

LEIGH TREACY
Partner
Head of Financial Services Advisory

+44(0) 7890 562 098
leigh.treacy@bdo.co.uk

LUKE PATTERSON
Partner, Internal Audit and Advisory
(PSR and EMI specialist)

+44(0) 7929 058 083
luke.patterson@bdo.co.uk

RICHARD BARNWELL
Partner, Regulatory and Advisory

+44(0) 7717 214 818
richard.barnwell@bdo.co.uk

ZAHRA ELLAHI
Senior Manager

+44(0) 7884 117 743
zahra.ellahi@bdo.co.uk

CONTENTS

Click each section to read more

1 2022 FCA Regulatory Priorities and Regulatory Grid

2 Financial services and Markets Bill – changes proposed to the UK financial services regulatory landscape

3 International Regulatory Landscape

4 IA Planning for 2022/3

5 Safeguarding Update

6 Economic Crime Update

7 The New Consumer Duty

8 Cyber Security: Social Engineering - what are the key risks and observations?

9 Operational Resilience and Outsourcing

10 Crypto Regulatory Update

11 ESG and Climate Change Update

12 UK Government's Response to Audit Reform: What does this mean for Internal audit?

13 The Intrinsic Link Between Diversity and Inclusion and Board Effectiveness

14 Round-up from the Regulators

2022/23 REGULATORY PRIORITIES

FCA Business Plan

Since the FCA's Business Plan was published in April 2022, the need to focus on the cost of living crisis has also become a regulatory priority. The FCA has issued a number of communications to firms reminding them of their obligations under the Pandemic Tailored Support Guidance to provide forbearance to consumers, lend affordably and ensure vulnerable consumers achieve the same standard of outcomes. The 2022/23 business plan has been grouped around three areas and relevance to Payments and E-money firms has been detailed below:

REDUCING AND PREVENTING SERIOUS HARM - FOCUS ON PROTECTING CONSUMERS FROM HARM THAT AUTHORISED FIRMS CAN CAUSE, INCLUDING TACKLING FRAUD AND POOR TREATMENT.	1. Dealing with problem firms. Under this topic heading FCA intends to take tougher interventions on firms that do not meet threshold conditions. The FCA announced on 19 May 2022 that a change in the law means it can cancel firms permissions if permissions are not being used. 2. Improving the redress framework. This is a wide ranging topic spanning how CMCs operate, requiring improvements to firms' own complaint handling process and reducing the burden of redress from liabilities accumulated by insolvent firms. 3. Reducing harm from firm failure. This is an ongoing topic to ensure firms have sufficient financial resources and are able to wind down in a way that causes the least amount of harm to consumers or other market participants. Focus on adequate safeguarding arrangements will be maintained. 4. Improving the oversight of Appointed Representatives. FCA Final Rules were published on 3 August 2022 and sets out requirements for firms to improve oversight of their Appointed Representatives. 5. Reducing and preventing Financial crime is maintained as a priority. This includes continuing focus on anti money laundering controls in firms and a new focus on 'Authorised Push Payment Fraud'. 6. Delivering assertive action on market Abuse. Much like Financial crime, this is a continuing theme where FCA will continue its surveillance of market abuse or failures to meet corporate disclosure requirements and take action.
SETTING AND TESTING HIGHER STANDARDS - FOCUSING ON THE IMPACT THAT AUTHORISED FIRMS' ACTIONS HAVE ON CONSUMERS AND MARKETS.	1. Putting customers needs first is a significant policy them for the FCA with the publication of flagship regulation in the new Consumer Duty. The FCA wants a step change in how firms deliver and enable good outcomes for consumers. Final Rules and guidance were published on 29 July 2022. Regulation of Buy Now Pay Later ('BNPL') now looks likely to be consulted on later in 2023. 2. Enabling customers to help themselves focuses on financial promotions with a call to firms to increase the quality of promotions, FCA will take tough action on illegal promotions and reduce the number of consumers investing in high risk investments. The FCA published its final rules for changes to the promotion of high risk investments on 1 August 2022. 3. ESG has a broad regulatory strategy to support Government policy and includes corporate disclosures, promotion of investments. This is a substantial agenda item where FCA is working with Government, other bodies and International regulators. Under this topic the FCA released final rules on diversity and inclusion requirements for firms on 3 April 2022. 4. Operational Resilience remains a core area of continued focus by FCA for example during the authorisation process. Firms should maintain services and ensure they are resilient to disruptions.
PROMOTING COMPETITION AND POSITIVE CHANGE - USING COMPETITION AS A FORCE FOR BETTER CONSUMER AND MARKET OUTCOMES.	1. Preparing financial services for the future post Brexit will be a fundamental look at the framework for financial services. The FSM bill laid before Parliament in July sets out the beginning of the multi years change journey. 2. Strengthening UK's position in global financial markets – the FCA has published consultations on wholesale market reforms (July 2022) on the back of Government consultation. FCA has also initiated market studies. These will inform and shape future changes to the regulatory framework for wholesale markets. 3. Shaping digital markets to achieve good outcomes. Along with Government and other regulators FCA is working on the future digital regulatory framework that will support competition and growth as well as enable good consumer outcomes.

HMT, FCA, PRA and other UK regulators contribute to a Regulatory Initiatives Grid setting out the combined regulatory initiatives affecting the financial sector which can be found here *Financial Services Regulatory Initiatives Forum*

FINANCIAL SERVICES AND MARKETS BILL

ALISON BARKER
Special Adviser

+44 (0) 7920 284 146
alison.barker@bdo.co.uk

The new FSM bill was laid before Parliament on 20 July 2022. Debates on the new proposals will not start until September. The bill is a significant piece of legislation running to over 300 pages and the largest financial services bill for 20 years. Its most significant purpose is to enable a comprehensive UK based financial services regulatory regime post Brexit and sets the framework for repeal and replace EU regulations (retained EU law). It provides new objectives and powers for financial regulators, who are not able to amend EU regulations. Strategically it is aimed at maintaining and growing the UK as a global financial services centre, fostering innovation and supporting the agenda for levelling up in the UK.

It will take some years for regulators to work through the body of retained EU law. In the majority of cases normal policy making processes will be followed with proposals for change put forward in consultation with the normal cost benefit analysis.

CHANGES FOR REGULATORS

New objectives for the FCA and PRA

In a drive to make UK financial services more attractive long term, both the PRA and FCA will have growth and international competitiveness as objectives as well as 'have regard to' climate change and net zero targets when discharging regulatory functions. Competitiveness is not to be prioritised above financial stability or consumer protection.

There are changes that make regulators have greater accountability to Parliament, strengthen the function of statutory Panels including placing the Listing Panel on a statutory basis and to create a Cost Benefit Advice panels. HMT will have power to direct regulators.

► What will be the impact?

This is a substantial and wide ranging piece of legislation which will be the start of more detailed changes from regulators. For firms, this will mean changes to be implemented over a number of years. It remains to be seen how much change is quickly initiated.

WHAT SHOULD PAYMENT SERVICES AND E-MONEY FIRMS BE THINKING ABOUT?

Legal and Compliance functions should be preparing for a period of change and maintaining an ongoing impact assessment to monitor proposals and impact of changes, especially in relation to the crypto payments space.

MAIN AREAS OF CHANGE RELEVANT FOR PAYMENT SERVICES AND E-MONEY FIRMS

- Crypto payments and changes to the EMI and payment services regulations. A framework for regulating crypto in the UK is lagging behind other jurisdictions. The bill brings activities facilitating the use of certain stable coins used for payment within the regulatory perimeter. Further Government consultation on crypto assets used as investments is expected later in 2022.
- A new Designated Activities Regime which will allow activities not compatible with the scope of FSMA legislation to be included. An example would be short selling. Powers are provided to FCA to set out how the activity should be carried out and to enforce.
- Financial promotions. The existing financial promotions regime is complex and has proved difficult for the FCA to regulate resulting in misleading promotions of complex financial products. Proposals for tightening the regime will mean that those firms wishing to approve promotions of unauthorised firms will require permission from FCA. Firms will be restricted to approvals within their sphere of expertise.
- Critical Third Parties – the legislative framework for the new CTP regime is set out giving HMT powers to designate critical third parties. A Discussion Paper was jointly released by regulators providing thoughts on the new regulatory framework.
- Securitisations – changes that enable HMT to designate jurisdictions as equivalent enabling non UK securitisations to be classed as 'simple, transparent and standardised (STS). This means they can be available in the UK under the STS securitisation regime to UK investors.
- APP scams – the Payments Systems regulator will be given powers to require mandatory reimbursement by payments systems providers to consumers subjected to authorised push payment fraud

OTHER CHANGES PROPOSED

- Insurance. The UK will be able to revoke existing Solvency II EU regulation and implements a new regime for insurers in financial difficulty.
- Access to cash – There are concerns that closing branches or some free to use ATMs means consumer access to cash or deposit facilities is becoming restricted. The bill sets out provisions for HMT to designate firms to be subject to FCA oversight to ensure the provision of cash is maintained.

Continued

FINANCIAL SERVICES AND MARKETS BILL (CONT.)

- Credit Unions – the bill enables changes to the activities Credit Unions can carry on which paves the way for changes recommended as part of the Woolard review to create a more sustainable unsecured credit market.
- MiFID - Nine changes to the MiFID II framework: (1) Removing the Share Trading Obligation; (2) Replacing the pre-trade transparency waiver regime and removing the Double Volume Cap; (3) Changing the definition of a systematic internaliser; (4) Removing restrictions on midpoint crossing for trades; (5) Aligning the Derivatives Trading Obligation with the EMIR Clearing Obligation; (6) Exempting for post-trade risk reduction services from the DTO; (7) Giving the FCA a permanent power to modify or suspend the DTO; (8) Simplifying the transparency regime for fixed income and derivatives; (9) Simplifying the position limits regime.
- Another area of retained EU law change will be the powers for UK regulators (BOE and FCA) to oversee financial market infrastructure which is had been a preserve of EU regulation. Provisions are also set out to apply the SMCR regime to FMIs and credit rating agencies.

INTERNATIONAL LANDSCAPE

ZAHRA ELLAHI
Senior Manager

+44 (0) 7884 117 743
zahra.ellahi@bdo.co.uk

BACKGROUND

Historically, banks have been at the centre of cross border payments, led by some dominant players with little disruption or competition. This has been shaken up over the last few years with a rush of new participants, looking to ease the pinch points of high costs, long settlement delays, accessibility and inefficient process with respect to cross border transactions. New players in the market have come in without the burden of legacy infrastructure and can gain a competitive advantage, resulting in rapid growth which creates its own problems.

The landscape for payments and e-money products internationally has become more and more fragmented and competitive with companies focussing on different geographies, transaction types and payment segments. What is clear is that Payments and E-Money firms are operating cross boarders and are needing to manage and operate under multiple regulatory landscapes.

CHANGING NEEDS

In addition, rapidly changing customer needs means consumers are looking for fast and intuitive services, and are unwilling to pay for services bank providers offer. The increasing use of smartphones and digital access has meant alternative solutions can be created on a faster, cheaper and more transparent platform.

EMERGING MARKETS

There has been a growing focus on emerging markets in the payments space with significant increases in the international transactions for Africa, Latin America and Asia. This has been supported with initiatives such government-mandated digital ID and close monitoring of the internet, factors that dramatically reduced the incidence of fraud via digital payments and improved consumer confidence from the outset. India's population and use of mobile devices, coupled with significant support from the Indian government and proactivity with regards to digitisation has led to increased accessibility for the unbanked and rural populations. Such investment has seen this market continue to attract attention and growth.

The UK and Europe has also seen a large growth in e-money institutions over recent years, many of these have been active across Europe thanks to "passporting" regime. Following the withdrawal of the UK from the European Union, the nature of the relationship with the EU has changed and many UK-based companies have already set up European entities and licenses, relocating their European Customers to European Territories (e.g. Ireland, Belgium, Lithuania, Latvia and Luxembourg).

We have seen payments and e-money institutions in particular, working closely with the Central Bank of Ireland (CBI) and Financial and Capital Market Commission (FCMC) in Latvia to build a European presence. Utilising the tools such as a regulatory sandbox, increased support and government initiatives to attract new entrants to the international regulated market, there has been a marked increase in interest and authorisation at these institutions.

We have also seen other European regulators increasing their focus on payments and e-money institutions, currently with regards to Safeguarding and intra group outsourcing. However, the increased scrutiny and oversight will force the multi territory firms to formalise process and controls where they operate a hub and spoke model of operations.

WHAT SHOULD PAYMENT SERVICES AND E-MONEY FIRMS BE THINKING ABOUT?

- Formalisation of process, control and reporting with regards to Safeguarding and Intra Group Outsourcing.
- With the implementation of the UK FCA's Consumer Duty, the drive to understand consumer needs and products is evermore important, including any products and pricing.
- Considerations to the use of international mediums of operation and digital enablement are driving innovative business models forward.
- Global relationships and networks enabling PIs and EMIs to offer far reaching products and services can impact operational resilience and risk management.

INTERNAL AUDIT PLANNING FOR 2022/23: UK SECTOR'S HOT TOPICS

LUKE PATTERSON
Partner

+44 (0) 7929 058 083
luke.patterson@bdo.co.uk

The August / September period is typically audit planning season and each year seems to have even more issues and developments for consideration than the previous year.

Key to risk-based auditing is prioritising the high risk areas for the IA team's activities over the coming year and assessing, with the help of an assurance map, where other assurance providers in the firm can be relied upon, and coordinated, to appropriately provide oversight and assurance to the Board to maximise the firm's resources.

Below is a thematic capture of a selection of the UK hot topics that IA teams within payments and e-money firms should include as part of wider considerations for the audit plan. Almost all of the issues have been examined in this pack and its previous monthly editions (please do get in touch if you need prior articles); but lets first discuss best practice for the planning process.

WHAT DOES EFFECTIVE AUDIT PLANNING LOOK LIKE?

- **Risk Assessment**: fundamental to the planning process is a documented risk assessment of the firm-wide risks that could impact the firm's strategic objectives, with an articulation of the risks' impact and likelihood, to help prioritise risks. A risk heat map is ideal to visually capture the risk assessment for Board consumption and provide rationale for resource allocation on specific aspects of the audit universe (do remember, its impossible, and inefficient, to attempt to audit everything).
- **Think annual, update quarterly**: the concept on a once-and-done annual plan is fast becoming obsolete. To keep nimble to the firm's strategic objectives, which have to adapt to the continually evolving business, risk and regulatory landscape, its advisable to have an annual risk assessment inform an annual plan (the "trajectory") and updates incorporated on a rolling quarterly basis (the "tweaks"), or sooner for high risk / material issues, to ensure internal audit continuously adds value throughout the cycle.
- **Mapping the firm's assurance framework:** Internal Audit will likely be one of many other internal and external assurance providers for the firm's control framework, therefore owning the firm's assurance map and keeping it up to date can help plan the IA activities to complement (not duplicate) the assurance work of other specialists. Enhancing this aspect of the process to consider a 3-year horizon of the firm's assurance needs will also support the firm's transition into the BEIS-led audit reform requirement for an Audit and Assurance Policy (if threshold criteria are met).
- **Bring the business in**: audit planning must incorporate the expectations of senior management, therefore its important to schedule discussions early on with the business unit heads and examine their perspectives as risk owners. Facilitation of a control self assessment by the IA team, ahead of the planning process, could help unearth a wider set of issues and risks not yet captured by risk oversight teams. Maximising feedback from employee engagement surveys could also help identify risks closer to the frontline.
- **CIIA FS Code**: use of the CIIA's Financial Services Code of Practice (2021) should be considered as a benchmark of good practice and factored into the planning process. The Code should be applied proportionately, and therefore smaller firms should apply the principles on which the Code is based in light of the firm's size, risk profile and complexity of operations.
- **Benchmarking**: how does your planning process compare to industry peer teams? Discussion of current and best practices, within the sphere of industry and trade body forums (e.g., CIIA, UK Finance), can help introduce improvements. This is especially the case for open-ended aspects of your planning process, e.g., how much of all engagement planning and fieldwork should aim to use data analytics?

ECONOMIC CRIME INCLUDING FRAUD RISK	SAFEGUARDING	CHANGE MANAGEMENT / PROJECT SPECIFIC	HORIZON SCANNING (E.G. SM&CR)
OUTSOURCING / THIRD PARTY RISK	CYBER / INFORMATION	CONDUCT RISK / CONSUMER DUTY	CLIMATE AND ESG
OPERATIONAL RESILIENCE	REGULATORY REPORTING	SWIFT PAYMENTS	MANAGING RESOURCE GAPS

SAFEGUARDING

TIANA RAVIRANJAN
Senior Manager

+44(0) 7870 540 710
Tiana.raviranjan@bdo.co.uk

SAFEGUARDING – A BRIEF BIT OF BACKGROUND

On the 29 November 2021 the FCA published PS21/19: Changes to the SCA-RTS and to guidance in the Payments and E-money Approach Document and the Perimeter Guidance Manual. This builds up upon and finalises earlier published guidance and consultations on amendments issued in January 2021 'Changes to the SCA-RTS and to the guidance in 'Payment Services and E-money – Our Approach' and the Perimeter Guidance Manual'. These proposals form part of the 2021/22 FCA Business Plan, to make the payments sector more resilient and protect consumers if firms fail.

In July 2021 the FCA published temporary guidance on safeguarding and prudential risk. This strengthened payment and e-money firms' arrangements in the exceptional circumstances of the pandemic and the FCA believed this would continue to be helpful (including post-pandemic) and therefore continue to be of the view that it should become permanent and thus are implementing the guidance largely as proposed, but with some clarifying amendments.

The main areas considered were:

- Expectations of an annual audit
- Clarifications on changes in business model
- Clarity on acknowledgement letters
- Guidance on notifications to the FCA
- Clarifications on the start and end points of the safeguarding obligations
- Guidance on the use of the insurance or comparable guarantee method
- Cost benefit analysis

SAFEGUARDING AUDITS

The FCA confirmed they expect auditors to provide a reasonable assurance opinion addressed to the firm on:

- whether it has maintained adequate organisational arrangements to enable it to meet our expectations of its compliance with the safeguarding provisions in the EMRs or PSRs, throughout the audit period, and
- whether it met those expectations at the audit period end date.

This expectation includes the need to provide an opinion regarding controls throughout the audit period, in addition to compliance at the audit period end.

The FCA did not mandate the use of a specific framework, although acknowledging that some respondents proposed the application of ISAE (UK) 3000. They also acknowledged that in the longer term there may be scope to develop a bespoke audit standard here.

They also stated that if an e-money or payment firm is required to arrange an audit of its annual accounts under the Companies Act 2006, it should arrange a safeguarding audit and ensure this work is completed as soon as reasonably practicable, with the expectation that given the initial safeguarding guidance published over a year ago they expect firms to have made significant progress with their safeguarding audits. It is also worth noting that that even if you are not required to have a safeguarding audit the FCA still expects those firms to have controls and processes in place to ensure customer funds are safeguarded.

No further definite clarity was obtained in respect of audit periods and timelines for completion however they did note that some firms may wish to align the audit period with their account year end and that this may mean, for example, setting an audit period end date of 31 December and arranging for an audit opinion to be submitted to the firm's management within 4 months of the audit period end date.

Continued

SAFEGUARDING (CONT.)

TIANA RAVIRANJAN
Senior Manager

+44(0) 7870 540 710
tiana.raviranjan@bdo.co.uk

CHANGES IN BUSINESS MODEL

When a firm changes its business model in a manner that materially impacts its safeguarding arrangements, the FCA consider an additional audit will be necessary and this would apply, for example, to an EMI that starts carrying on payment services unrelated to issuing e-money.

It was clarified in the FCA's Approach Document that this will entail sharing a report prepared by an independent auditor in line with a reasonable assurance engagement, with the FCA and that the report should state the auditor's opinion on the firm's systems and controls and whether they are suitably designed to comply with relevant safeguarding regulations. The expectation is that this opinion will be shared with the FCA in a reasonable period in advance of the firm adopting new safeguarding arrangements in line with its obligation to notify the FCA of a change in circumstances under Regulation 37 of the PSRs and EMRs.

ACKNOWLEDGEMENT LETTERS

The FCA also noted that where a firm can't obtain an acknowledgment letter from their safeguarding credit institution or custodian, they must still be able to demonstrate that the safeguarding credit institution or custodian has no interest in, recourse against, or right over the relevant funds or assets in the safeguarding account and that this should be clearly documented, and agreed by the relevant credit institution or custodian, for example, in the account terms and conditions.

A notification to the FCA should be made when Firms are unable to comply with safeguarding requirements.

The FCA also provided additional examples in the Approach Document of when they would expect to be notified if a firm has not or is ~~are~~ unable to comply with safeguarding requirements. These included:

- failure to keep up to date records of relevant funds and safeguarding accounts,
- inability to resolve any reconciliation discrepancies in the way described in paragraph 10.88
- the decision by an authorised credit institution or authorised custodian to close a safeguarding account
- failure to carry out reconciliation as frequently as appropriate
- **Start and End points of the safeguarding obligation**

Further clarity was also provided on the start and end points of the safeguarding obligation with the FCA reiterating that EMIs should not treat relevant funds, that they are required to safeguard, as being available to meet commitments to card schemes and other third parties but instead starts as soon as the institution receives the funds.

Whilst also reiterating that the safeguarding obligation remains in place until the funds are no longer held by the payment or e-money institution.

INSURANCE OR COMPARABLE GUARANTEE

Earlier guidance was issued in respect of this and it was agreed that this earlier guidance would be consolidated within the approach document as well as applying this to the guarantee method of safeguarding. This included the below additions to the approach document:

- the amount of the insurance cover or comparable guarantee must at all times include reasonable headroom to allow for any foreseeable variation in the amount of the safeguarded funds being protected by the insurance policy or comparable guarantee
- there should be no level below which the insurance policy or comparable guarantee does not pay out
- the insurance policy or comparable guarantee should provide cover for at least as long as the institution is using insurance or a comparable guarantee to protect the safeguarded funds
- the institution must ensure that their insurer or guarantor understands that the circumstances that led to a claim would provide no grounds to dispute their liability to pay it

WHAT SHOULD PAYMENT SERVICES AND E-MONEY BE THINKING ABOUT?

In terms of next steps, we recommend reviewing the adequacy and suitability of current audits undertaken or planned as well as current systems and controls in line with the changes noted above and published in PS21/19 as well as version 5 of the approach document.

Our reviews to date have shown particular areas requiring further focus to be:

- **Formalisation of policies and procedures,**
- Reconciliations and breach reporting, and
- IT controls over systems used within the Safeguarding process.

ECONOMIC CRIME UPDATE – NCA RED ALERT ON FINANCIAL SANCTIONS EVASIONS

DECLAN BIDDULPH
Manager

+44(0) 7974601788
declan.biddulph@bdo.co.uk

NCA RED ALERT ON FINANCIAL SANCTIONS EVASION TYPOLOGIES: RUSSIAN ELITES AND ENABLERS

In July 2022, the National Economic Crime Centre (NECC), a multi-agency unit in the National Crime Agency (NCA), and HM Treasury's Office of Financial Sanctions Implementation (OFSI), working in conjunction with law enforcement and financial sector partners as part of the Joint Money Laundering Intelligence Taskforce (JMLIT), issued a 'Red Alert.' The purpose of the 'Red Alert' is to provide information from law enforcement and the legal and financial services sectors about common techniques designated persons (DPs) (individuals and entities subject to financial sanctions) and their UK enablers are suspected to be using to evade financial sanctions.

WHAT DOES THE 'RED ALERT' SAY?

The 'Red Alert' explains how some DPs are using a range of techniques in order to evade sanctions impacting on their personal and commercial holdings. This activity is occurring shortly before the imposition of sanctions or soon after. DPs are transferring or selling assets, sometimes at a loss, and divesting investments to reduce ownership below 50% or relinquish controlling stakes.

A DP may claim to have relinquished the asset, but the 'Red Alert' states that it is highly likely that they will retain their influence through trusted proxies and enablers. Enablers are individuals or businesses facilitating sanctions evasion and associated money laundering. Key enabler professions include:

- Legal (barristers and solicitors)
- Financial (relationship managers, accountants, investment advisors, wealth managers, payment processors, private equity, trust and company service providers)
- Estate agents
- Auction houses
- Company directors, Intermediaries/agents and private family offices

The 'Red Alert' lists 34 indicators for the detection of frozen asset transfers, detection of enablers and the detection of suspicious payments. Many of these cover existing risks like the abuse of trust structures, holding companies located offshore or in jurisdictions historically linked to the Soviet Union, and transactions by holding companies linked to DPs with Swiss bank accounts and BVI/Cypriot legal persons. The 'Red Alert' also mentions payments from offshore jurisdictions, the Middle East, East Asia or jurisdictions that still support the Russian government or express neutrality in international forums like the UN.

In terms of what appear to be emerging trends the 'Red Alert' notes the risk of payments via a Fintech (e.g. a payment service provider or e-money institution) with Russian investor nexus. This could include customer transactions that are initiated from or sent to IP addresses that have non-trusted sources, or are located in Russia, Belarus, jurisdictions with FATF-identified Anti-Money Laundering (AML) deficiencies or comprehensively sanctioned jurisdictions.

WHAT INDUSTRY RECOMMENDATIONS DOES THE 'RED ALERT' MAKE?

The 'Red Alert' specifies six recommendations, which firms should consider:

- Arms-length transactions need to be documented and should not be taken at face value by firms. If they have any doubt, firms are advised to seek guidance from OFSI.
- Paying particular attention to source of wealth and source of funds checks, especially if conducted by third parties.
- Making a careful assessment of complex corporate structures as a key component of enhanced due diligence on high-risk customers.
- Issues of aggregation of ownership can be further complicated where differing approaches to aggregation of ownership are applied across the EU, UK and US and more than one owner seeks to divest their shareholding. Firms are advised to seek guidance from OFSI if in doubt.
- Where firms are presented with documentation that purports to present a change in ownership by a company linked to a DP, it is important not only to conduct enhanced due diligence, but to follow up with the relevant competent authority (OFSI in the UK) to understand if firms have reason to believe that ownership has not been transferred appropriately.
- When companies have provided their own legal assessments regarding the transfer of ownership, firms should also carry out their own legal assessment in order to come to their own determination.

The 'Red Alert' also reminds us that, as a tool of foreign policy, UK sanctions have jurisdiction both over England, Wales, Scotland and Northern Ireland, as well as the Crown Dependencies and Overseas Territories (which includes the British Virgin Islands). Further, all UK persons worldwide are required to comply owing to the extra-territorial application of the Sanctions & Money Laundering Act 2018.

ECONOMIC CRIME UPDATE - ARE YOU READY FOR THE UPDATED MONEY LAUNDERING REGULATIONS

DECLAN BIDDULPH
Manager

+44(0) 7974601788
declan.biddulph@bdo.co.uk

THE MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT)(NO.2) REGULATIONS 2022

On September 1st 2022 the Money Laundering and Terrorist Financing (Amendment)(No.2) Regulations 2022 is due to come into force and therefore, payments services firms and e-money institutions will need to comply with the amended regulations from this date.

WHY ARE THE REGULATIONS AMENDING?

The government conducted a consultation between July and October 2021 to invite views on how to strengthen the Money Laundering Regulations, with the results of the consultation and the amendments to the Money Laundering Regulations currently sitting before Parliament for approval. The amendments have been implemented to make time-sensitive updates to ensure the UK continues to meet the international standards set by the Financial Action Task Force, whilst also ensuring the UK's anti-money laundering regime is operating effectively.

The key amendments to the regulation for payments services firms and e-money institutions include:

- Firms will need to include Proliferation Financing in addition to money laundering and terrorist financing in their risk assessments and where the risk assessments identifies inherent proliferation financing, firms will need to ensure they have policies, procedures, and systems and controls to mitigate such risk;
- Regulation 30a will require firms to report discrepancies in beneficial ownership information to Companies House for ongoing business relationships, extended from when establishing a business relationship;
- The amended regulations will see Account Information Service Providers be excluded from the scope of Money Laundering Regulations due to the service acting as an information tool rather than coming into possession of customers funds, therefore having a much lower risk of money laundering and terrorist financing.

WHAT DOES THIS MEAN FOR YOU?

- A risk assessment should be conducted to assess your proliferation financing inherent risks and where exposure is identified, you must ensure adequate policies, procedures, and systems and controls are in place to mitigate such risk.
- Policies and procedure must be updated to take in consideration the updated requirements of Regulation 30a. Training must also be provided to staff with a responsible of conducting ongoing monitoring of clients to ensure that in the event a discrepancy in beneficial ownership is identified, this is reported to Companies House.
- Those who are classified as Account Information Services Providers, despite no longer being subject to the Money Laundering Regulations, must continue to consider their wider money laundering, terrorist financing and sanctions inherent risk exposure and determine their obligations under relevant legislation such as the Proceeds of Crime Act 2002.

Whilst we have highlighted the key amendments to the Regulations that will impact payments and e-money institutions, we encourage firms to review the amendment in full to ensure that come 1st September 2022, all the relevant updates policies, procedures, and systems and controls are enhanced and up to date.

FCA'S CONSUMER DUTY – FINAL RULES AND GUIDANCE

ALISON BARKER
Special Adviser

+44 (0) 7920 284 146
alison.barker@bdo.co.uk

The FCA has published the much-anticipated final rules for new Consumer Duty. This is a step change in consumer regulation to create higher standards for consumers and improving competition in the retail financial services market. It is complex and wide ranging.

The Consumer Duty aims to improve the outcomes for retail consumers including small and medium sized enterprises, setting clearer and higher expectations for firms' standards of care towards consumers by acting in good faith and avoiding foreseeable harm, and supporting customers in reaching their goals. It goes much further than previous initiatives under Treating Customers Fairly.

A NEW PRINCIPLE AND NEW RULES AND GUIDANCE

The structure is unchanged from earlier consultations with a new Principle, three cross cutting rules and rules relating to four outcomes. Final Guidance provides examples and further detail.

The wording of the new Principle 12 will be ' a firm must act to deliver good outcomes for retail customers'. Existing Principles 6 and 7 will be disapplied where the Consumer Duty Principle applies but will be retained to apply to activities outside the Consumer Duty.

The cross-cutting rules provide more clarity on interpreting the new Principle and Rules and require firms to:

1. act in good faith toward retail customers
2. avoid foreseeable harm to retail customers
3. enable and support retail customers to pursue their financial objectives

FOUR OUTCOMES

The four outcomes represent key elements of the firm-consumer relationship to help ensure a comprehensive approach to achieving good consumer outcomes. Firms will need to understand and evidence how outcomes against each of these are being met. The four outcomes are:

Communications – getting communications to consumers at the right time to equip customers to make effective, timely and properly informed decisions about financial products and services.

- **Products and Services** – to be designed to meet the needs of consumers; are sold to those whose needs they meet; and perform as expected.
- **Customer service** – that meets the needs of consumers, enabling them to realise the benefits of products and services and act in their interests without undue hindrance.
- **Price and Value** – to ensure that the price of products and services represent fair value for consumers.

DEADLINES FOR IMPLEMENTATION

These have changed and are phased. Firms will now have 12 months to 31 July 2023 to implement the new rules for all products and services currently on sale. The rules will be extended to closed book products (those that are no longer on sale) 12 months later for implementation by 31 July 2024.

The extension of the deadline for products and services currently on sale is good news as many firms have been struggling to implement by the original deadline of April 2023.

To ensure firms are focused on delivery, FCA has required Boards to sign off on implementation plans by end of October 2022 and maintain ongoing oversight of delivery. This is a change and ensures Boards are sighted on progress. FCA supervisors will be asking to see evidence of Board scrutiny. Boards are still required to attest that they meet the standards at the end of the implementation period.

Manufacturers are required to share information with distributors by 30 April 2023 so that distributors can complete their implementation in time for the July deadline.

WHAT SHOULD PAYMENT SERVICES AND E-MONEY FIRMS BE THINKING ABOUT?

The Final Guidance sets out examples and more detail for firms. Of note is the guidance to Payment Services firms and EMI's about the application of the Consumer Duty to them. FCA has confirmed the Consumer Duty will apply in full. Payments firms and EMIs need to think about their distribution chains and FCA has particularly called out communications, advertising, and servicing as key areas of focus.

Continued

FCA'S CONSUMER DUTY – FINAL RULES AND GUIDANCE (CONT.)

ALISON BARKER
Special Adviser

+44 (0) 7920 284 146
alison.barker@bdo.co.uk

WHAT WILL BE THE IMPACT?

- This regulation is anticipated to raise standards and firms need to be prepared for scrutiny from FCA on how they are implementing the new requirements. Timescales are tight with a phased implementation over two years. Many firms were waiting for final rules before starting projects and will now have a short period to get implementation plans ready for Board scrutiny by end of October.

  Internal Audit functions should have Consumer Duty impact assessment and implementation plans in scope to provide assurance to the Board that the firm is able to meet the implementation timescales.

  FCA supervisors will seek evidence of Board scrutiny. Boards are still required to attest that they meet the standards at the end of the implementation period. Therefore, IA teams should evaluate evidential sources of information of the Board's scrutiny over implementation plans, i.e. Board and committee discussion minutes, impact assessments produced by second line oversight functions, risks flagged by frontline teams – have these been incorporated into firm-wide risk assessment?

  Facilitating a Risk and Control Self Assessment, including all the functional areas to be impacted by the new Consumer Duty, could help unearth a number of issues to better inform the preliminary risk assessment for a review of Consumer Duty implementation.

CYBER SECURITY: SOCIAL ENGINEERING – KEY RISKS AND OBSERVATIONS

DANIEL HILL
Assistant Manager

+44 (0)7812 467 445
daniel.hill@bdo.co.uk

Given the constant cyber and physical security risks facing all financial services firms as they seek to protect their client data, it is imperative that firms continue to develop their best practice standards. "Social engineering" has proven to be a successful route for criminals to penetrate data security controls. External attackers typically manipulate a firm's employees by exploiting their behavioural responses to fraudulent communications and illegitimately obtain sensitive information, thus breaching the firm's data protection requirements, and potentially damaging the firm's reputation.

The global COVID-19 pandemic, and the ongoing transition to hybrid working patterns, has further intensified the risks from social engineering. We take a look, below, at some of the most common social engineering tactics identified from our internal audit co-source controls testing in recent weeks.

PRETEXTING

Pretexting is impersonation by the social engineer of a legitimate stakeholder to the firm in order to obtain sensitive information. In some cases, it can be undertaken by creating a 'trustworthy' identity over a period of time, thereby creating a plausible scenario for manipulation of staff. A typical example of pretexting we have observed is a criminal impersonating a client of the company and seeking the full names and contact details of senior staff members in preparation for a future attack.

DUMPSTER DIVING

Dumpster diving is, literally as the term suggests, looking for sensitive information within a firm's waste disposal process. The nature of the discoveries may appear trivial in isolation, for example, staff member lists, technical support logs, etc.; however, taken together, an attacker can build an effective profile of an employee (or team) with which to target for a future social engineering attack.

EMAIL PHISHING

Email Phishing is a technique of sending emails, from apparently reputable sources, with the aim of gaining personal or corporate information. Phishing can involve the embedding of an attachment within an email that loads malware onto a computer or a link to an illegitimate website that can trick an employee into handing over personal information. Common forms of malicious emails include:

- Current events and charities (i.e. testing whether details have been compromised in a recent data leak);
- Technical support (i.e. the need for urgent password renewal);
- Financial institutions (i.e. your bank asking for your details to provide an update).

PHYSICAL INTRUSION

Intrusion is when the attacker physically enters the building or property of the firm in order to obtain sensitive information (e.g., through abandoned documents and 'shoulder surfing') or to connect a rogue device physically to the internal IT network. Absent or overloaded reception / security staff, particularly at peak morning hours, is a straightforward route through which a criminal can bypass physical controls.

CASE STUDY: OUTPUTS FROM A RECENT SOCIAL ENGINEERING REVIEW OF AN FS CLIENT

Phishing – throughout a social engineering email campaign we tested on the client's employees, a substantial number of employees clicked on malicious phishing links with some providing their full usernames and passwords and not flagging a risk to IT security

During physical intrusion testing, discrepancies were found in security processes:

- No requirement to scan an ID badge to get into the office building;
- No ID or badge swipe/tap was required to gain access to the building floors;
- No concierge/attendant monitoring the office entrance space; and
- Upon inspection of conference rooms, we found cards detailing the Wi-Fi login for guests. Our internal audit team confirmed that these Wi-Fi passwords were correct as our testing team were able to illegitimately connect to the firm's networks.

WHAT SHOULD PAYMENT SERVICES AND E-MONEY BE THINKING ABOUT?

- Is sufficient training in place to ensure staff are aware to remain vigilant against both phishing attacks and physical intrusion, is the training regularly performed (at least annually) and regularly updated to incorporate new and dynamic criminal tactics?

Continued

CYBER SECURITY: SOCIAL ENGINEERING - KEY RISKS AND OBSERVATIONS (CONT.)

DANIEL HILL
Assistant Manager

+44 (0)7812 467 445
daniel.hill@bdo.co.uk

- Are adequate Cyber/IT and Physical security policies and procedures in place, such as a clear desk policy, and are they embedded within the firm's control environment, i.e. "tone at the top" continues to reiterate the importance of such controls, the firm's culture incorporates cyber and physical security risks across all activities, etc.?
- Is there sufficient investment in the firm's IT and physical security controls to keep pace with the dynamic nature of the associated risks, e.g. two factor identification of clients, and an independent security penetration testing programme in place for early detection of the firm's vulnerabilities?
- Has the Internal Audit team factored in the CIIA's latest technical guidance for Social Engineering related reviews (found within the CIIA's IT Auditing and Cyber Security members' webpage) and do IA colleagues have sufficient training to carry out such reviews? Has an appropriate specialist advisor been factored into the skills matrix of the IA activity in preparation for future security reviews / penetration testing?

OPERATIONAL RESILIENCE AND OUTSOURCING

KARUNA BHANDERI
Associate Director

+44 (0) 758 367 6111
karuna.bhanderi@bdo.co.uk

OUTSOURCING – A BRIEF BIT OF BACKGROUND

- Outsourcing and use of third-party suppliers is widespread as firms seek to reduce costs, increase efficiency and benefit from external expertise to perform certain functions. However, outsourcing as an activity does not outsource the risk related to that activity. Whilst some risk is inherently transferred to the third party, the ultimate ownership and accountability of the outsourced service rests with the regulated firm, particularly when the activity is related to the fulfilment of a regulatory obligation.
- The FCA have set out clear expectations in relation to outsourcing arrangements within section 8 of the FCA Senior Management Arrangement, Systems and Controls ("SYSC") Handbook.
- Where relevant, PIs and EMIs must consider these requirements. Outsourcing arrangements are detailed for PIs and EMIs specifically in Regulation 26 of the E-money Regulations 2011 and Regulation 25 of the Payment Services Regulations 2017.

OUTSOURCING AND OPERATIONAL RESILIENCE

- The FCA issued Policy Statement 21/3 regarding operational resilience in March 2021, applicable to PIs and EMIs, which adds a further layer of complexity to Outsourcing and Operational Resilience.
- PIs and EMIs need to fully consider and identify Important Business Services, Impact Tolerances, Transitional Arrangements and Mapping and Scenario Testing as a means of enhancing their operational resilience framework.
- Firms are required, where they have any third-party suppliers responsible for the delivery of a firm's "Important Business Service", to have such suppliers:
  - Included within the firm's operational resilience mapping;
  - Assessed for their potential risks as outsourced service providers;
  - Assure the firm, to the extent the firm relies on the supplier's own testing, on the suitability of the methodologies, scenarios and considerations adopted by the third-party to carrying out testing of it's operational resilience.
- The FCA has confirmed that if firms are unable to obtain sufficient information and assurance from the third party supplier to satisfy themselves that the third party can operate within the determined impact tolerance(s), then the firm should review and, if necessary, change its outsourcing arrangements.
- While firms have until March 2025 to complete their Operational Resilience mapping with a view to be able to remain consistently within their board-approved impact tolerances, such conversations with third-parties can present a challenge where third-party relationships are potentially complex, deeply rooted, long-standing or intra-group (i.e. outsourcing to entities within the parent structure).
- The FCA have been clear that firms cannot delegate their regulatory responsibility to another party. A relevant act or omission by another party to which a PI or EMI has outsourced activities will be an act or omission by the PI or EMI itself.

BACK TO BASICS

- The mapping exercise and assessment of vulnerabilities undertaken as part of Operational Resilience requirements rely on a clear and robust outsourcing and third-party risk management framework to support a complete assessment.
- We have seen a number of firms making improvements to their existing frameworks to facilitate a deeper understanding of their reliance on third party vendors and the potential risks to the firm's resilience from continued reliance on outsourcing arrangements.

WHAT SHOULD PAYMENT SERVICES AND E-MONEY BE THINKING ABOUT?

- **Programme managers**: The FCA has highlighted that all e-money issuers, including those authorised under FSMA, should consider the use of programme managers for issuing of prepaid cards will fall under the outsourcing provision in regulation 26 of the EMRs or SYSC 8 for credit institutions. E-money issuers need to ensure all conduct of business requirements are complied with.

Continued

OPERATIONAL RESILIENCE AND OUTSOURCING (CONT.)

KARUNA BHANDERI
Associate Director

+44 (0) 758 367 6111
karuna.bhanderi@bdo.co.uk

- **Assurance Reviews**: Where not already planned, Outsourcing and Third-Party Framework internal audit reviews would support the ongoing work required during the transition period. The FCA believe they have provided an appropriate amount of time to allow firms to embed the changes that may be necessary within their business, including to make appropriate investment to help embed operational changes. It should also be noted that the March 2025 is a hard deadline and a firm that is not making reasonable effort to remain within its impact tolerances during this time would be in breach of the FCA's rules.
- **Tone at the Top**: As a firm's impact tolerances become better understood and socialised, there is an expectation that they are fully embedded and discussed at appropriately senior forums in a similar manner to risk thresholds, albeit retaining an awareness that they are driven by different objectives. Assurance teams should evaluate whether Operational Resilience discussions have continued, at Board level, beyond the March 2022 milestone and how resilience has been embedded within the enterprise-wide risk framework, i.e. how have the firm's risk management processes developed as a result of assessing, mapping and better managing resilience and outsourcing risks?

ECONOMIC CRIME UPDATE – CRYPTOASSETS

CLARINDA GRUNDY
Senior Manager

+44 (0) 7901 133290
clarinda.grundy@bdo.co.uk

FCA ANNUAL REPORT AND ACCOUNTS 2021/22

In August 2022, the FCA published its Annual Report and Accounts which, amongst other things, highlighted the continued need for regulated entities to proceed with caution with respect to cryptoassets. In particular, it notes that only 33 cryptoasset firms had successfully passed through its Temporary Registration Regime ("TRR") as of the Regime's conclusion on 31 March 2022. Further, it warns firms that the FCA has identified over 200 crypto firms which continue to trade despite being FCA-supervised.

WHAT DOES THIS MEAN FOR YOU?

The cryptoasset domain continues to be turbulent, and there remain potential challenges with respect to misuse of novel and electronic virtual currencies for sanctions evasion as well as money laundering and terrorist financing. Firms should therefore keep in mind that:

- While the 33 cryptoasset firms which have been through the TRR now sit within the FCA's regulatory perimeter, these firms are newly regulated and should still be subject to risk-based due diligence controls
- If engaging with the cryptoasset sector, firms should be particularly probing of the flow of value, gaining a comprehensive understanding of the source of funds ("SOF") and evaluating whether this makes commercial sense. Firms should be particularly cognisant of cryptoasset activity emanating from jurisdictions with weaker compliance frameworks or which have flown through mixing, tumbling or other obfuscation services
- There remains a large portion of the cryptoassets sector which is unregulated and operates without supervision. Firms should pay particular attention to these, applying robust due diligence measures before the commencement of a business relationship to gain comfort that the cryptoasset company, its beneficial owners, its business activities and its fund flows are legitimate.

GLOBAL FINES CONTINUE FOR POOR ANTI-MONEY LAUNDERING ("AML") CONTROLS IN CRYPTO FIRMS

On 1st August 2022, the New York Department of Financial Services ("NYDFS") levied a fine of $30m USD against Robinhood Crypto LLC ("Robinhood") for alleged AML failings, predominantly relating to the firm's Governance and Oversight and transaction monotiling ("TM") processes and controls. Robinhood is a trading platform which enables registered users to convert their USD fiat currency into virtual currencies and undertake cryptocurrency trades.

DEFICIENCIES IN ROBINHOOD'S AML CONTROLS NOTED BY THE NYDFS

The NYDFS had investigated Robinhood covering the operating period 24th January – 30th September 2019 and found the following gaps in the Firm's AML framework:

- Over-reliance of Robinhood on the compliance program of its parent company, without sufficient oversight from and tailoring to the specific entity operating in USD;
- Lack of sufficiently skilled staff to operate the firm's AML program;
- Inappropriate TM provisions, whereby a manual-only system remained in despite the firm's alert volume increasing by 500% and thresholds for investigation were arbitrary and set too high; and
- Backlogs in processing alerts, particularly with respect to evaluating potentially suspicious transactions to determine whether a suspicious activity report ("SAR") should be filed.

The NYDFS enforcement action also cites that, during the assessment time period, the Firm failed to demonstrate the expected compliance culture with respect to its cryptoasset activities. This, in addition to the failings noted above, was deemed by the NYDFS to lead to poor observed engagement with the Regulator.

WHAT DOES THIS MEAN FOR YOU?

This latest fine evidences that, despite being supervised, there remains propensity for deficiencies in firm's AML frameworks. It is therefore critical that any firm seeking to onboard a cryptoasset firm should ensure to conduct robust due diligence measures prior to commencement of the business relationship. This should include both identifying and verifying the entity itself as well as gaining a degree of comfort with respect to the company's own AML processes and controls.

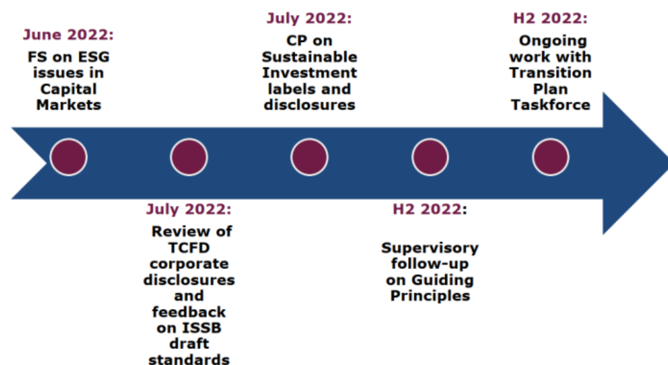
ESG AND CLIMATE CHANGE UPDATE

GLORIA PEREZ TORRES
Manager

+44 (0)7583 689 198
gloria.pereztorres@bdo.co.uk

TASKFORCE ON NATURE-RELATED FINANCIAL DISCLOSURES LAUNCHED

- The Taskforce on Nature-related Financial Disclosures ("TNFD") is a new global market-led initiative which seeks to provide financial institutions and corporates with a complete picture of their environmental risks and opportunities.
- The TNFD will design a risk management framework for banks to report and act on evolving nature-related risks, building on the success of the Task Force on Climate-related Financial Disclosures (TCFD). The TNFD framework is intended for use globally by corporates and financial institutions of all sizes.
- Whilst the final version of the framework is expected for 2023, banks and financial institutions are encouraged to become familiar with the framework and consider how these will be incorporated into the wider TCFD framework of the organisation.
- The framework will help banks and financial institutions to manage both shorter-term financial risks (deemed material today), as well as longer-term risks presented by nature-related dependencies and nature impacts.
- Firms should expect to receive a set of recommendations and guidance on TNFD disclosures, which will be used to document their assessment on how they will implement the recommendations within their frameworks.
- The drafted recommendations will require firms to publish a statement of the scope of disclosures and what will be covered in future disclosures, based on four pillars:



WHAT SHOULD PAYMENT SERVICES AND E-MONEY BE THINKING ABOUT?

- There aren't specific regulatory requirements for the payments and e-money sector, as there are for banks, insurers and asset managers, but it is clear the FCA expects all regulated firms to show leadership in this area.
- PIs and EMIs may start thinking about ESG in the context of seeking investment – be prepared to answer questions from investors about things like embedding diversity
- Start to link your ESG considerations to your business strategy

FCA'S KEY ESG MILESTONES FOR 2022

Alongside the Bank of England and PRA's 10-part pledge for its climate agenda, to facilitate its prudential supervision of ESG priorities, the FCA is also further developing its conduct supervision agenda to ensure all aspects of ESG are embedded in everything it undertakes, from authorisations to supervision, through its 5 steps plan:

1. High-quality corporate disclosures: Ensure they get the right information and for organisations to reflect on how they look at sustainability risks.
2. Active investor stewardship: Focusing on accountability.
3. Effective ESG ecosystem: Holistic approach to data and disclosures and legal services, etc.
4. Sustainable investment labels: To support clients to make appropriate decisions, and to help firms for labelling, classification and fund disclosure requirements.
5. ESG Embedded in FCA regulation: e.g. ESG ratings.

What we can expect in H2 2022:

UK GOVERNMENT'S RESPONSE TO AUDIT REFORM: WHAT DOES THIS MEAN FOR INTERNAL AUDIT

BRUK WOLDEGABREIL
Associate Director

+44 (0)7467 626 468
bruk.woldegabreil@bdo.co.uk

A QUICK REFRESH FOR OUR MEMORY – WHAT'S HAPPENED SO FAR?

- In March 2021, the Department for Business, Energy and Industrial Strategy (BEIS) published a "white paper" to consult on proposals for an overhaul of the audit sector. Suggested measures, amongst a number of proposals, included:
  - Reducing the market concentration of the largest audit firms;
  - Increasing the accountability of corporate directors in the UK's largest firms;
  - Creation of a new regulator for the audit industry, the Audit, Reporting and Governance Authority (ARGA) and introduction of new internal control reporting requirements.
- On 31 May 2022, BEIS published its response to the consultation. While the emphasis of the government's proposals address statutory (external) audit services, there is likely to be a substantial impact on the Internal Audit activity of public interest entities (PIEs).

WHAT ARE THE KEY PROPOSALS FROM THE CONSULTATION RESPONSE?

- **ARGA**: the new statutory regulator will replace the Financial Reporting Council and have new powers, including the ability to direct companies to restate their accounts without going to court. ARGA will also be able to investigate and sanction directors of large firms for breaches of duties around corporate reporting and audit;
- **Definition of PIEs**: the scope will expand to include large unlisted companies (with more than 750 employees and £750 million annual turnover) adding an estimated 600 companies within the remit of ARGA;
- **Audit scope**: premium listed PIEs will be required to explain how they assure the quality and reliability of information in their annual reports outside the financial statements, including on climate change, risk management, and internal controls;
- **Reporting requirements**: introduction of a new statutory "Resilience Statement" and an "Audit and Assurance Policy" (more on this for IA teams, below) to improve reporting of the firm's risk management and degree of assurance put in place. The UK Corporate Governance Code will require company directors to attest to the effectiveness of a firm's internal controls and the basis of its assessment;
- **Market competition**: a new 'managed shared audit' regime will be introduced on a phased basis. FTSE 350 companies will have to appoint a challenger auditor outside of the "Big Four" or allocate part of their audit to a smaller firm.

WHAT SHOULD PAYMENT SERVICES AND E-MONEY BE THINKING ABOUT?

- The starting point is the CIIA's position paper, following the consultation response, which flags the "Internal Audit Call to Action" alongside each of the proposed requirements put forward to facilitate audit reform in PIEs.
- **Audit and Assurance Policy (AAP)**
  - An AAP articulates what independent assurance, if any, the firm intends to obtain in the next three years in relation to the annual report and other company disclosures beyond that required by statutory audit;
  - The AAP would explain the independent assurance in place for the firm's Resilience Statement, internal controls framework, and a description of the firm's internal auditing and assurance processes, as well as policies for tendering statutory (external) audit services;
  - Internal audit teams have a key role in facilitating and supporting the creation of the firm's AAP. The CIIA has already published technical guidance on what should be considered for an AAP, how to facilitate creation of an AAP and best practice examples taken from the recent annual reports of PIEs.
- **Resilience Statement**
  - The new Resilience Statement will replace the existing Viability Statement and Going Concern disclosure;
  - This Resilience Statement will also require at least one stress-test and the role for internal audit would be to independently review, verify, and audit the narrative of the Resilience Statement in terms of accuracy and transparency, prior to it being formally submitted to the statutory auditor.
- **Premium listed firms: Internal Controls**
  - The UK Corporate Governance Code is expected to be strengthened, in its next update, to require an explicit directors' statement about the effectiveness of the company's internal controls and the basis for that assessment;
  - IA teams within premium listed firms will need to collaborate with first and second line assurance providers to strengthen their internal controls related to financial reporting;
  - All other PIEs, outside of this requirement, may consider this incoming reform as an opportunity to voluntarily establish a benchmark for internal controls.

THE INTRINSIC LINK BETWEEN DIVERSITY AND INCLUSION AND BOARD EFFECTIVENESS

JENNIFER CAFFERKY
Senior Manager

+44 (0)790 5716994
jennifer.cafferky@bdo.co.uk

BACKGROUND

The FCA has published its highly anticipated Policy Statement, "(PS22/3) Diversity and Inclusion requirements for Boards and Executive Management", following a Consultation Period which closed in October 2021.

This Policy Statement, marks the first requirement by the FCA for in-scope firms (those subject to the FCA's Listing Rules) to formally report on Diversity and Inclusion (D&I) data within their annual financial reports.

However, the Policy Statement did not necessarily come as a surprise, given how vocal the FCA has been on the topic of D&I over a number of years. For example, in July 2021, the FCA published a Discussion Paper, "Diversity and inclusion in the financial sector - working together to drive change" jointly with the Bank of England and PRA. This Discussion Paper explored how the Regulators can make financial services more diverse and inclusive.

The FCA also, at the same time, published a review of research literature regarding the impact of D&I in the workplace (and particularly looking at the impacts of D&I on business performance, risk management, and conduct outcomes). D&I is also referenced within the FCA's Business Plan (for 2022/23), both in terms of enhancing D&I within the FCA itself; as an employer, and a public body, and in terms of how it engages with, and regulates firms.

The FCA has clearly been assessing how it can further incorporate D&I into its regulatory regime in a substantive and meaningful way. This Policy Statement feels like the natural next step - in terms of setting more concrete benchmarks for firms around diversity and inclusion.

WHAT DOES THE REGULATOR EXPECT TO SEE?

For firms who are in-scope of the new requirements (i.e., PS22/3), they will be required to make specific disclosures in their annual report as to whether they have met specific D&I benchmarks. These requirements will be in place from financial years starting on 1 April 2022 (or sooner, if firms wish, on a voluntary basis). The benchmarks are summarised in our previous update.

These benchmarks will be implemented on a "comply or explain" basis. This means that these benchmarks are not formal requirements, but targets, with the FCA acknowledging that there is a need for some flexibility. However, firms will need to provide an explanation as to why they haven't met the benchmarks, and there is likely to be some challenge if the explanation is not robust enough.

WHAT DOES THE POLICY STATEMENT MEAN FOR OUT OF SCOPE?

The Regulator has been clear that its latest Policy Statement serves only as a starting point. The FCA has already said that it intends to review the new Policy in 3 years' time to assess its impact. This will include considering whether to amend the nature or level of the targets, and whether to include targets on wider aspects of diversity.

It is, therefore, highly possible that other firms may be brought within scope and will need to adhere to the benchmarks in due course. It is also possible that the FCA will look to include new benchmarks or reporting requirements regarding other aspects of diversity (e.g., social mobility, disabilities, LGBTQ+), and/or that current benchmarks may be increased (e.g., increasing the number of women on Boards to 50%).

Diversity and inclusion is one of the top agenda points for the Regulators, and it should subsequently be a top agenda item for firms both within and beyond the scope of PS22/3. Firms should also not be engaging with this topic purely from a "benchmark" perspective. The Regulators will be expecting firms to truly engage with the topic, and what it means, and how it can benefit each firm and the customers or clients it services.

WHAT ARE SOME OF THE KEY CONSIDERATIONS FOR INTERNAL AUDIT TEAMS WHEN THE SENIOR MANAGEMENT SEEKS TO INCREASE BOARD DIVERSITY AND ULTIMATELY BOARD EFFECTIVENESS?

A few key points for the Chief Audit Executive and the IA activity to consider:

1. Enhancing Board diversity and inclusiveness, should not just be a case of firms trying to meet benchmarks. Recruiting or selecting a Board member or Executive should not be based on filling a category without considering whether and how the individual can add value. Solely focusing on numbers will likely not positively impact Board effectiveness or meet the spirit of what the Regulators are trying to achieve.

A ROUNDUP FROM THE REGULATORS

REGULATOR	DATE	DOCUMENT	WHAT'S NEW?
FCA	19/08/22	Letter to British Retail Consortium about Buy Now Pay Later (BNPL) firms [PDF]	Letters to British Consortium and CEOs about misleading advertising for Buy Now Pay Later products
FCA	27/07/2022	PS22/9	A new Consumer Duty: FCA's final rules
FCA	27/07/2022	FG22/5	A new Consumer Duty: FCA's final guidance
PRA	22/07/2022	CP13/22	Amendments to the PRA's approach to identifying other systemically important institutions (O-SIIs)
EBA	22/07/2022	Report	EBA publishes report on use of specific exemptions included in the large exposures regime
FCA/PRA/BoE	21/07/2022	DP22/3	Operational resilience: critical third parties to the UK financial sector
HMT	21/07/2022	Call for Evidence	HMT consultation on Payments Regulation and the Systemic Perimeter in response to the government's 2021 'Payments Landscape Review'
FCA/PRA/BoE	21/07/2022	Dear CEO letter	Transforming data collection – an update on progress and plans for 2022
PRA	20/07/2022	Speech	New tides – speech by Nathanaël Benjamin regarding the risks and challenges for investment banks

A ROUNDUP FROM THE REGULATORS (CONT.)

REGULATOR	DATE	DOCUMENT	WHAT'S NEW?
BCBS	15/06/2022	Principles	Principles for the effective management and supervision of climate-related financial risks
HMT	15/06/2022	HMT Response	HMT published the outcome of its consultation on amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
HMT	16/06/2022	HMT Announcement	UK government commits to reform of the Consumer Credit Act to cut costs for businesses and simplify rules for consumers
FCA	16/06/2022	Dear CEO letter	FCA wrote to 3,500 lenders, including retail banks and consumer credit firms, setting out expectations in light of cost of living pressures

CONTACTS

INTERNAL AUDIT
LUKE PATTERSON
Partner
luke.patterson@bdo.co.uk

RICHARD WEIGHELL
Partner
richard.weighell@bdo.co.uk

REGULATORY ADVISORY
RICHARD BARNWELL
Partner
richard.barnwell@bdo.co.uk

MADS HANNIBAL
Partner
mads.hannibal@bdo.co.uk

FIONA RAISTRICK
Partner
fiona.raistrick@bdo.co.uk

EXTERNAL AUDIT
KELLY SHEPPARD
Partner
kelly.sheppard@bdo.co.uk

ORLA REILLY
Partner
orla.reilly@bdo.co.uk

ACCOUNTING AND CORPORATE REPORTING ADVISORY
MARK SPENCER
ACRA Leader
mark.spencer@bdo.co.uk

TAX
DAVID BRITTON
Partner
luke.patterson@bdo.co.uk

R&D TAX CREDIT
CARRIE RUTLAND
Partner
carrie.rutland@bdo.co.uk

M&A
ISH ALG
Director, Mergers & Acquisitions
ish.alg@bdo.co.uk

FORENSICS
SIMON GREAVES
Partner
simon.greaves@bdo.co.uk

OUTSOURCING
ROBERT HUTCHINGS
Director
robert.huchings@bdo.co.uk

LUKE PATTERSON

+44 (0)7588 434 233
luke.patterson@bdo.co.uk

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright © October 2022 BDO LLP. All rights reserved. Published in the UK.