IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

June 2024

BDO FS INTERNAL AUDIT CONTACT POINTS

BDO's Banking & Building Societies Update summarises the key regulatory developments and emerging business risks relevant for all banks, building societies and, where flagged, for alternative finance providers (i.e., peer-to-peer lenders, card providers, E-money services providers and debt management companies).

Our FS Advisory Services team are working with more than 50 banks and building societies as internal auditors and advisors, giving us a broad perspective on the issues facing the sector. We have aggregated insights from our in-house research, client base, the Regulators and professional bodies, including the Chartered Institute of Internal Auditors (CIIA), to support your audit plans and activities.

We hope this pack provides value to you and your colleagues; please do share with us any feedback you may have for our future editions.

LEIGH TREACY
Partner

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

CHRIS BELLAIRS
Partner

+44 (0)7966 626 128
christian.bellairs@bdo.co.uk

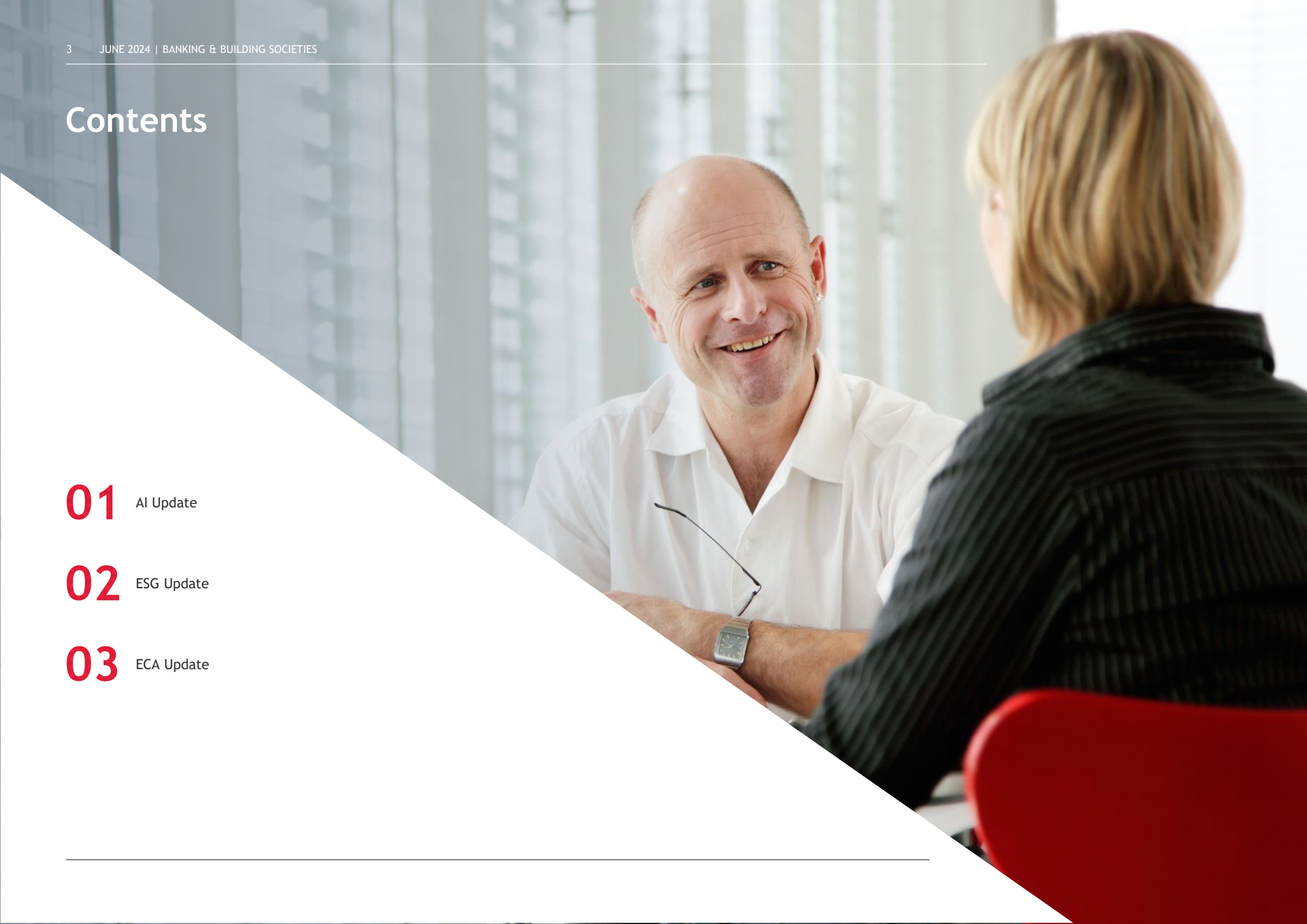
SAM PATEL
Partner

+44 (0)7970 807 550
sam.patel@bdo.co.uk

BRUK WOLDEGABREIL
Associate Director

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

Contents



01

Artificial Intelligence Update

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

Artificial Intelligence (AI): What are Regulators thinking about?

AI is the topic of the day, recent publications by Regulators give focus to some of the anticipated benefits, risks and challenges policy experts are considering. This article provides an insight into some recent publications by policymakers and their evolving thinking.

This debate will be of direct interest to Heads of Internal Audit who are engaging with their Boards about the broader benefits and risks of AI as part of IA's horizon risk scanning.

Overview

The Competition and Markets Authority (CMA) is concerned with generative or foundation models, and deep learning AI models that can generate high quality content, like text or images, based on the data they were trained on. They are looking at the creation of these models and the risks to competition and innovation.

The FCA is considering the impact of Big Tech's entry into the financial sector, how they might disrupt traditional financial sector incumbents and the potential for good consumers outcomes plus the risks of market power of Big Tech.

The speech by Jonathan Hall, external member of the Financial Policy Committee (FPC) of the Bank of England, is considering the risks to financial markets from deep trading algorithms. The FPC's role is to examine and reduce the risks of financial instability in the UK financial system. He sums up AI models as follows:

"An artificial neural network is an information processing system. It converts inputs into outputs via a series of hidden layers, the nodes of which are connected with different weights, which are optimised through a training process. The greater the number of layers, the more complex the input-to-output operation and the harder the network is to understand and predict. A network with more than 3 layers is usually called a deep neural network. Chat GPT-3 has 96 layers and 175 billion parameters."

The CMA perspective: What is generative AI and why is the CMA looking at it?

Sarah Cardell, Chief Executive of the CMA, outlined three risks from generative AI in a speech in April 2024, launching a CMA report about technical report into AI Foundation Models (FMs).

The transformation and progress of models like Chat GBT are described as a 'whirlwind' by the CMA.

The CMA is interested because this technology could be transformational for businesses and consumers in the UK, but it also carries risks. It is concerned that a small number of incumbent technology firms are shaping the development of AI in ways that could have a detrimental effect on competition in the UK. It has identified three risks to innovation and competition:

- Firms control critical inputs for developing foundation models to shield themselves from competition.
- Powerful incumbents exploit their position to restrict choice in foundation models services or deployment.
- Partnerships across value chains exacerbate existing market power.

The CMA CEO commented:

"Specifically, we believe the growing presence across the foundation models value chain of a small number of incumbent technology firms, which already hold positions of market power in many of today's most important digital markets, could profoundly shape these new markets to the detriment of fair, open and effective competition, ultimately harming businesses and consumers, for example by reducing choice and quality and increasing price."

The CMA's most recent report considers the guiding principles for developing AI to ensure positive competition and consumer protection outcomes. The guiding principles confirmed by CMA are as follows and they can be found in the full report. These guiding principles form the basis of the CMA's perspective.

The question for FS firms, is what these developments mean for financial sector development and deployment of AI?

FCA's focus on Big Tech

The FCA's two most relevant objectives here are consumer protection and promoting competition in the interests of consumers. FCA commentary is focused on how firms can safely and responsibly adopt the technology as well as understanding what impact AI innovations are having on consumers and markets. The FCA says it is "technology agnostic." AI has the potential to bring new products and services to retail consumers and greater efficiencies to markets such as open platforms or a tool for financial advice. It is a more optimistic view of the potential for AI than that of the CMA.

Artificial Intelligence (AI): What are Regulators thinking about?

Linked to the development of AI, is the potential impacts of Big Tech entry and expansion in retail financial services. The long-term risks of Big Tech (by which FCA means Google, Amazon, and Meta etc) in retail financial services are their market power. The market power of these firms has the potential to innovate and create new offerings or value for retail consumers using tools such as AI, challenging incumbent financial sector firms. But long term, that market power could also become detrimental because of their ability to entrench their own positions. These are the risks the CMA is monitoring.

The FCA predicts partnerships between Big Tech and traditional financial sector providers as the most likely route. Although Amazon has found entry into the insurance market difficult and has closed Amazon Insurance, which partnered with a number of UK insurers, after only two years. It shows the difficulty new entrants face in financial services markets.

What should Internal Audit teams think about?

In a speech interestingly entitled "Monsters in the Deep" Jonathan Hall, considered two ways in which rapidly developing AI models could pose a risk to financial stability. He was discussing the use of Deep Trading Algorithms which are deep neural networks/large language models in developing in wholesale markets. Internal audit teams should consider these risks for any audit planning on AI and related topics.

The first risk is that neural networks as traders may be very efficient short term, but create brittle and highly correlated financial markets, unable to absorb shocks. This in turn creates the circumstances for unstable and less resilient financial markets. Examples of systemic market risks from trading algorithms is not new, for example high frequency trading and the value of circuit breakers on trading venue platforms. For example, the flash crash in 2010 when the Dow Jones Industrial Average dropped 1,000 points in 10 minutes, losing $1 trillion in equity values, although most of that was recovered by the end of the day.

The second risk is that neural networks learn from each other. Partly this is down to the way trading strategies need to consider the strategies of other players and partly because they are built to learn. Trading Algorithms focused on maximising profit may do so at the expense of stability – will they know when to stop? At first this may seem to be an optimising strategy; however, it can lead to risks of herd behaviour, colluding behaviour, or behaviours that fail to respect regulation such as market abuse regulation. Looking again at his definition of deep neural networks, their complexity and opacity could make these features difficult to identify. Mitigation strategies are discussed, including very close monitoring to spot errant behaviour in the AI.

The effects of deep trading algorithms and the interaction with market abuse regulation are perhaps an area for greater consideration by the Third Line, particularly given the FCA's role in market surveillance.

02

ESG Update

ADAM SOILLEUX
Director

adam.soilleux@bdo.co.uk

GLORIA PEREZ TORRES
Associate Director

gloria.pereztorres@bdo.co.uk

Taskforce on Inequality and Social-related Financial Disclosures

With climate change having been a priority for national and international regulatory frameworks in recent years due to its urgency, social and inequality related issues (often referred to as the "S" pillar within ESG) haven't been as highly prioritised by regulators within the UK financial services sector to date. Whilst some firms already conduct social impact reporting with reference to the Sustainable Development Goals or the GRI Standards, for example, these broader frameworks are mostly voluntary and are not currently aligned. It has, therefore, been difficult for stakeholders to draw meaningful comparisons, and firms which are subject to other regulatory pressures may have been prioritising any mandatory risk assessments and associated reporting.

What is TISFD and what is its purpose?

The TISFD (Taskforce on Inequality and Social-related Financial Disclosures) is "a global initiative to develop recommendations that enable businesses and investors to effectively identify, assess, and report on their inequality and social-related risks, opportunities, and impacts". It will also advise on the interlinkages between climate change, biodiversity loss, and social issues, to guide market actors in contributing to a just transition.

The requirement is expected to be launched in September 2024 and internal audit teams should have this in mind for 2024/25 annual planning if ESG assurance reviews will be scoped.

The TISFD Working Group has published a proposed governance structure and technical scope of the TISFD, to which BDO is in the process of responding.

What are the TISFD proposals?

The TISFD will provide guidance, thresholds, targets, and metrics for companies and investors to measure and manage their impacts on inequality, as well as inequality's impacts on company and investor performance.

What should Internal Audit teams think about?

With authorised firms now being expected to meet the anti-greenwashing rule, and prepare for other regulatory requirements in the pipeline, there is a growing number of ESG requirements to keep track of for audit planning.

Based on the current proposals, TISFD will provide a much-needed structure which will support firms in identifying, measuring and reporting on their inequality and social-related impacts, dependencies, risks and opportunities.

Whilst the final details of the framework are not yet known, as UK financial services firms often operate on a global scale, the alignment of TISFD with other global standards will contribute to more streamlined reporting across different jurisdictions, reducing the complexity and cost of compliance and potentially its assurance.

Internal Audit teams should monitor the publication of the TISFD framework, guidance and recommendations, alongside other current ESG-relate developments, so that the incoming requirements can be considered as part of planning for ESG reviews, but also to consider how such criteria regarding social factors could be integrated thematically into other relevant audit reviews, e.g., Culture.

03

Economic Crime Update

CLARINDA WOODFORD
Associate Director

clarinda.woodford@bdo.co.uk

Economic Crime Update

UK Government publishes its UK Financial Sanctions FAQs

On 8 May 2024, the Office of Financial Sanctions Implementation ('OFSI'), part of HM Treasury within the UK Government, published an update to its FAQs.

There are 91 FAQs in total, grouped under 12 categories (such as Russia, Libya etc), which are intended to be supplementary to, and not a replacement for, OFSI's primary guidance.

The OFSI publication indicates that one of the FAQs has been updated in May – question 1 (category – General) "How do I stay informed about new designations?". In response OFSI advises that people can subscribe to OFSI's e-alerts service via the OFSI website which provides helpful updates on designations and important changes.

In addition, the Foreign, Commonwealth and Development Office ('FCDO') also operates an e-alerts service which provides updates on designations, important changes, policy changes and press releases.

Appropriate tracking of legislative and regulatory requirements, such as subscription to these alerts, should be included in reviews over Second Line monitoring activities.

What should Internal Audit teams think about?

Given the current and ongoing geopolitical tensions, it remains vital for firms to stay abreast of (UK) sanctions developments to ensure they remain compliant. Second Line teams should periodically refresh themselves on the content of the FAQs, as well as OFSI's primary guidance, and calibrate their sanctions frameworks accordingly.

Third line assurance activities should focus on the following, non-exhaustive, examples of control areas with respect to reviews on sanctions compliance:

- Ensuring that evolving sanctions risk exposures are adequately identified and assessed in the firm's business wide risk assessment ('BWRA');
- Maintaining an up-to-date and accessible Sanctions Policy;
- Calibration and monitoring of sanctions screening tools, both with respect to name and payment screening;
- Refining alert investigation and disposition protocols to ensure that narratives are clear and standalone;
- Maintaining rigour with respect to sanctions list management;
- Developing robust escalation channels for internal reporting of (potential) sanctions breaches, including generation of appropriately granular and timely management information ('MI');
- Proactively reporting externally (to OFSI, and potentially wider) as needed when sanctions breaches are identified; and
- Ensuring that staff undergo regular general sanctions training and tailored, as well as role specific training for staff with particular responsibilities/remits.

HM Treasury publishes its annual report on anti-money laundering and counter-terrorist financing ('AML/CFT') supervision

On 1 May 2024, HM Treasury published its latest annual report on anti-money laundering and counter-terrorist financing ('AML/CFT') supervision. As required by the Money Laundering Regulations, the report provides information about the performance of the UK's 25 AML/CFT supervisors' performance between 6 April 2022 and 5 April 2023. This includes the Financial Conduct Authority ('FCA'), UK Gambling Commission ('UKGC'), HMRC as well as the 22 Professional Body Supervisors ('PBSs').

Highlights from the report's chapter on the FCA's supervisory activity are as follows:

- Retail banking (including payments), wholesale banking, wealth management and crypto-asset firms remained particularly vulnerable to financial crime and posed the greatest risk of being exploited for money laundering;
- The number of desk-based reviews ('DBRs') has returned to pre-pandemic levels, with 231 taking place during the period. Less than half (103, 45%) were assessed as 'compliant'. Formal actions were taken in 9 instances following DBRs, and informal actions in 31 instances.
- In-person onsite visits have resumed since a hiatus during the pandemic – 7 took place during the period. None were assessed as 'compliant'. Formal actions were taken in 1 instance following onsite visits, and informal actions in the remaining 6 instances.
- Common issues of non-compliance identified by the FCA through DBRs and onsite visits included:
  - Inadequate client and firm-wide risk assessments
  - Insufficiently risk-sensitive or granular enhanced due diligence ('EDD') processes, leading to poor identification and monitoring of customers, such as Politically Exposed Persons ('PEPs')
  - Ineffective application of EDD which in turn leads to poor identification and monitoring of high-risk customers
  - Insufficient compliance monitoring, and insufficient quality assurance and testing programmes to assess operational effectiveness of systems as well as their design
  - Inadequate resources dedicated to, and training of staff responsible for compliance
  - Inadequate documentation of risk-assessments and measures taken to monitor risk.

Economic Crime Update

What should internal audit teams think about?

The HM Treasury report sends a clear signal that the FCA remains subject to high standards from the UK Government, and is expected to deploy its supervisory powers in an appropriate, proactive, data-driven and risk-based manner. This in turn means that firms within the FCA's supervisory pool should also expect to continue to receive intensive FCA scrutiny with regards to both the design and operating effectiveness of their AML/CTF controls.

The low levels of outcomes of 'compliant' based on the FCA's DBRs and onsite visits indicate that there is a significant way to go in truly operating a robust AML/CTF framework across all supervised entities. This leaves obvious gaps for criminals and illicit actors to exploit, reducing the safety and security of the UK as a place to do business.

Internal audit teams should regularly and objectively assess the strength of their financial crime frameworks in light of the Money Laundering Regulation, JMLSG Guidance, FCA Financial Crime Guide and other relevant guidance documents and make updates as required. This should include, but not be limited to, review of the Second Line's work in:

- Undertaking a formal BWRA, typically at least annually, and taking steps to de-risk or enhance controls based on the outcomes of this;
- Defining a clear risk-based approach with respect to due diligence, ensuring that all customers are appropriately risk-rated (at onboarding and throughout the relationship) and stricter measures are applied to higher risk customers commensurate to the risks posed;
- Ensuring that protocols for the identification and treatment of PEPs has been formalised, especially in light of the recent updates made to the Money Laundering Regulations relating to treatment of domestic vs foreign PEPs;
- Deploying a comprehensive compliance monitoring plan, linked to the BWRA outcomes, to provide assurance on the design and operating effectiveness of AML/CTF controls;
- Hiring and retaining resources with the right skillsets and experience to undertake key AML/CTF roles;
- Ensuring that staff undergo regular general AML/CTF training and tailored, as well as role specific training for staff with particular responsibilities/remits;
- Maintaining strict protocols regarding the expected granularity and detail required to be captured to articulate and justify risk decisions which have been taken.

UK Finance publishes its Annual Fraud Report 2024

On 21 May 2024, UK Finance (in partnership with Feedzai) published its Annual Fraud Report 2024.

With fraud-related losses standing at nearly £1.2 billion in 2023, the report highlights that fraud remains a "major problem and threat to the UK" and should be a key item on firms' radars.

While the report notes that steps have been taken to reduce fraud, such as implementing requirements for Strong Customer Authentication ('SCA') in e-commerce and the launch of the 'Take Five' national campaign, criminals continue to find innovative and sophisticated ways to dupe and trick individuals into parting with their money.

Some highlights included in the report include:

- There has been a significant growth in card ID theft (where a criminal uses a fraudulently obtained card or card details, plus stolen personal information, to open/take over a card account held in someone else's name). In 2023 losses relating to card ID theft were 53% higher than in 2022, and cases rose by 74%.
- Romance scams losses rose by 17% in 2023. This is where victims are persuaded to make payments to a person they have met (typically online) with whom they believe they are in a relationship
- Purchase scams attributed to authorised push payment ('APP') increased 28% in 2023, and more than 75% of APP fraud cases originate online.
- In 2023, £1.2b of unauthorised fraud was prevented, representing a 7% increase on the previous year. While this highlights the ongoing efforts from industry to reduce harm to consumers and prevent money from reaching criminals, there is still more to be done.
- Reimbursements rates are also on the rise, and this trend is expected to continue following consultation from the Payment Systems Regulator ('PSR') on mandatory reimbursement, which will come into force later this year.

What should internal audit teams think about?

Fraud continues to be an industry hot topic and, with ongoing challenges such as the cost of living crisis and enhancements in technology, there remains a real threat of fraudsters infiltrating and damaging lives.

If this alone isn't motivating enough for firms to continue to prioritise fraud risk management, the introduction of the new "failure to prevent fraud" offence as part of the Economic Crime and Corporate Transparency Act ('ECCTA') in 2023 has certainly reinforced its importance.

For firms in scope for the ECCTA, operationalising 'reasonable procedures' to prevent fraud is a must, and for those not it would be considered a good practice. Notwithstanding the wait for publication of guidance from the UK Government, which is now expected to be delayed in light of the announcement of the General Election, Third Line teams should consider the following activities in co-ordination with Second Line financial crime and

Economic Crime Update

compliance teams:

- Gaining buy in and top level commitment from the board of directors and senior management to develop and maintain a comprehensive and robust fraud risk management programme;
- Developing/updating a Business-Wide Fraud Risk Assessment to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks;
- Deploying tailored and proportionate anti-fraud policies and procedures to mitigate the specific fraud risks faced, as determined through the Business-Wide Fraud Risk Assessment;
- Documenting and operationalising preventative and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner;
- Ensuring that staff undergo regular general fraud training and tailored, as well as role specific training for staff with particular responsibilities/remits, to build awareness of potential red flags and how these should be identified, investigated and escalated; and
- Performing ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicating fraud risk management programme deficiencies in a timely manner to parties responsible for taking corrective action including senior management and the board of directors.

FOR MORE INFORMATION:

SAM PATEL

+44 (0)7970 807 550
sam.patel@bdo.co.uk

BRUK WOLDEGABREIL

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

www.bdo.co.uk

XXXXXXX