Best practices in combating fraud in financial institutions

Received in revised form 4th April, 2022

John Mahony
Head of Compliance and MLRO, Atrato Group, UK

John Mahony is Head of Compliance and MLRO at Atrato Group, an alternative asset investment advisory group, specialising in asset-backed income strategies. John has worked across the financial services industry, including investment managers, hedge funds, administrators and stock exchanges. He is a subject matter expert and regular speaker at industry roundtables and conferences.

Atrato Group, Fourth Floor, 36 Queen Street, London, EC4R 1BN, UK
E-mail: john.mahony@atratopartners.com

Abstract This paper intends to provide the reader with practical steps to take when establishing a framework for combating fraud.

Keywords: *best practice, internal fraud risk, corruption risk, combating fraud*

INTRODUCTION

Risk and compliance professionals have had to adjust risk and control frameworks and continuity plans during the pandemic while continuing to meet business as usual (BAU) requirements to protect clients, consumers and the market.

The pandemic has caused additional fraud vulnerabilities to emerge. The half-yearly report by UK Finance stated that "In the first six months of 2021, losses incurred as a result of investment scams rose by 95% compared to H1 2020 …",[1] while a report by Mazers[2] shows that prosecutions of company directors, financiers and CFOs jumped by 205 per cent in the year to 30th September, 2021.

Compliance and risk professionals are aware of and work to protect customers against external frauds, but financial institutions are certainly not immune to internal fraudulent activity taking place, particularly where there is a significant increase in opportunity factor as a direct result of the circumstances the pandemic brought about. Failure to identify fraud early could lead to potentially intolerable reputational risk.

This paper takes a broader legislative[3] approach to defining a 'financial institution' (referred to as a 'Firm' or 'Firms'), encompassing both PRA-authorised[4] persons and persons authorised by the Financial Conduct Authority ('FCA')[5]. The fraud risks affecting individual Firms will vary depending on a Firm's permissions, operational strategy and governance structures.

Surveys are continuously undertaken to determine the scale and cost of fraud within business more generally. Firms are included within the scope of such surveys but are not focused on in a meaningful way. Results vary significantly due to the scale and detail of the data set required to assess the true cost and risk posed to financial institutions. These surveys also pick up reported and disclosed cases, so that one could argue that detection is working to some extent, but it is the unreported frauds that are the issue. It must be stated that these surveys are valuable to compliance and risk professionals to review potential vulnerabilities in preventative control measures. For example, corruption risk has been highlighted as the highest risk to Firms, making up at least 40 per cent of reported cases.[6] Fraud risk is constantly evolving as a result of numerous externalities and Firm-specific circumstances. This highlights the need for consistent review and assessment of risk through an established framework.

OVERVIEW

Fraud is a criminal act that can be described as: (i) making a dishonest representation for personal advantage or to cause another a loss; (ii) dishonestly neglecting to disclose information when there is a duty to do so; (iii) abusing a position of power (for personal gain); (iv) false accounting (eg, misleading statements); or (v) conspiring with others to commit fraud (agreeing to do something that could cause loss to a third party).[7]

Although not all Firms are covered, the FCA's Financial Crime Guide[8] is a useful starting point for Firms wishing to assess the expectations for prevention, assessment of risks, systems and controls.

The criminal law will overlap with fiduciary and regulatory obligations that a Firm may have. Although we are not police officers, care should be taken to ensure policy breaches are not construed as a separate issue from criminal activity in any framework, particularly taking into account the corruption risk figure set out above. In order to effectively manage fraud risk, a Firm must consider the possibility that the law has most likely been broken as a result of a breach or of control failure due to internal factors, externalities or both.

Firms should undertake a phased approach to combating fraud depending on their compliance maturity level. In general, Firms should, at a minimum, have a robust risk and compliance framework with a scoring methodology, a system for standardising controls, a records management plan, a governance structure and an engaged governing body. This is not to say anti-fraud measures need to be at the same level of maturity.

There are many approaches that Firms can take to implement an Anti-Fraud Programme ('AFP'). Importantly, there is no one-size-fits-all approach, taking into account the size, scale and complexity of a Firm's business; therefore, it is appropriate to set out principle-based best practice that can be applied in way that suits individual Firm parameters.

GOVERNANCE AND CULTURE

Simply put, the Firm's governing body needs to define the outcomes and benefits it wants to achieve from the AFP. In order to be in a position to define the desired outcomes and benefits, management will have to provide the governing body with the Firm's AFP maturity level. Firms will have varying degrees of fraud exposure or risk appetite, which will drive both the current state and desired outcomes; it is up to individual Firms to assess their current state and the target state. Broadly speaking there are five levels of maturity (see Table 1).

Arguably, most Firms should, at a minimum, be at 'Actionable' maturity level or aiming for that in the short term. Once a maturity level has been determined, the Firm will need to address what steps are required to reach the target maturity level desired. This is best achieved through a strategy road map, which should include both short and long-term plans to achieve the target maturity, based on gaps identified. This can be achieved by pinpointing and prioritising the gaps between the current maturity level and the target maturity level. Table 2 will assist Firms in uncovering gaps.

Governance is vital to a well-structured AFP, but culture will be the determining factor of whether it is well-functioning or not. There is no doubt that everyone reading this will have heard the phrase 'tone from the top' ad nauseam, but it is fair to say choices are led by culture and a Firm's approach to cultivating the right one is awareness and engagement, which 'tone from the top' does not always deliver.

The most powerful fraud detection and monitoring tool any Firm has at its disposal is its personnel. The FCA has spoken about the concept of 'tone from within',[9] which may seem to many like a nebulous concept but it does allow for the engagement of all levels. Of course, governance structures are required and parameters for the acceptable level of risk must be set by leadership and reinforced by management but engagement, awareness and value alignment is needed to embed a culture.

Compliance and risk professionals should be acutely aware that systems and controls are prey to the rogue bad actor; the gap that should be monitored on the way to achieving best practice is the susceptibility of systems and controls being prey to individual assessments of risk that might be wrong,[10] often as a result of poor culture and awareness. There may be innumerable choices made by individuals within Firms in any given

Table 1:

1. Provisional

Fraud identification measures are not formalised, are characterised by a lack of fraud risk management, and are largely event driven and ad hoc. Requires individual effort.

2. Reactive

Fraud Identification measures are formalised but ad-hoc and managed in silos and are largely reactive and event driven.

3. Actionable

Formalised fraud identification measures are standardised and repeatable. The controls environment integrates with the risk programme. Fraud reports are reviewed by the governing body.

4. Managed

Formalised fraud identification measures have been integrated with performance and controls environment. Performance is measurable and can be analysed on a granular level. There is a defined notification procedure for changes in risk management.

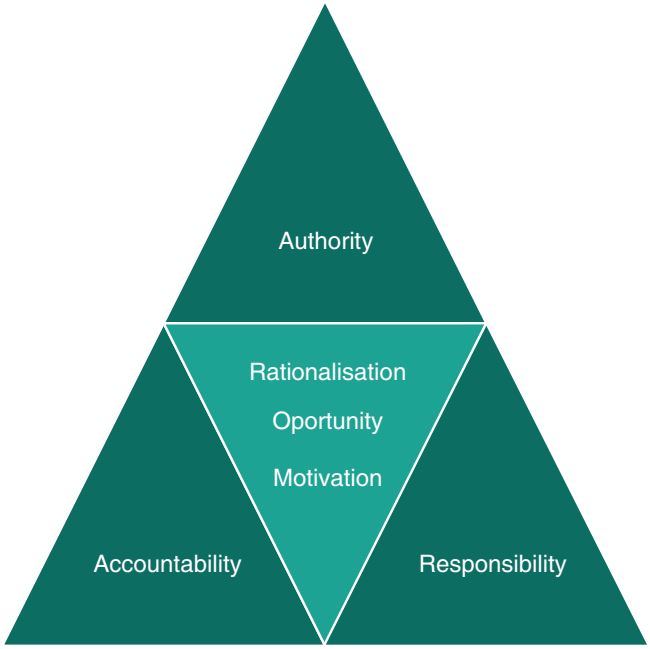
5. Strategic

Formalised fraud identification measures are continuously reviewed, changed, and improved. The entire programme is reviewed by the governing body, receiving regular reports with well-defined measurements against performance.

Table 2:

Headline	Considerations
Firm commitment	This should take into account the correlation between culture and fraud risk management and should assess the code of conduct standards as a deterrent.
Governance	The governing body should have a clear understanding of what constitutes fraud and should be composed of independent members, ensuring management maintains the AFP effectively.
Fraud risk management policy	The policy should be tailored to the Firm's risk profile, with relevant fraud risk scenarios communicated to personnel so that they know the consequences of fraud and understand how it affects their role.
Roles/responsibilities	Overall responsibility for fraud risk management should be assigned to a single executive-level individual who reports to the board.
Formalised AFP	The programme should define fraud, identify both internal and external potential perpetrators of fraud, provide hypothetical Firm-centric examples of fraud, and define the roles and responsibilities of those charged with oversight of fraud control.
Training/awareness	Augment fraud risk management policy with a periodic, mandatory, targeted fraud training course based on roles for all personnel. Establish accountability for all internal controls, including fraud risk management and fraud prevention and detection.

Table 3:



time period. No amount of controls will make all those choices binary 'yes' or 'no' responses without creating bottlenecks in service resulting in detriment to clients, the market or falling foul of some regulatory obligation.

The starting point for any Firm wishing to promote fraud awareness should be about the threat of fraud through targeted and sufficiently precise training. However, to embed a culture means providing personnel with a capacity to combat fraud, promoting individual accountability. The intended impact is to ensure that choices that cannot be made binary have accountability attached to them. Therefore, individuals making a choice have the authority to do so but remain accountable for it. This is most effective where awareness is high and there is an understanding of implications and consequences. The following diagram illustrates this point, whereby the components of the fraud triangle are neutralised when surrounded by Authority, Responsibility and Accountability (see Table 3).

In order for the method of embedding an anti-fraud culture to work effectively, Firms should periodically assess the effectiveness of fraud awareness practices, identifying any gaps over time. This might include conducting an annual employee survey to assess personnel's knowledge of the AFP (for example, how they report ethical concerns or misconduct and if concerns have been taken seriously). Firms should also continuously update training and test them against outcomes.

Embedding a culture will take time but early engagement of personnel in the risk process will ensure initial awareness of priorities. Personnel should be consistently engaged in the AFP by ensuring they are informed of any risks identified as they emerge.

PREVENTION

Fraud risk is a form of operational risk arising from inadequate or failed internal processes, systems, misconduct or adverse externalities. Sound fraud risk management controls should be designed to deter fraud or minimise its likelihood, while being commensurate with the size, complexity and risk profile of a Firm. A fraud risk assessment should be undertaken to identify gaps and potential opportunities for improvement in key operational areas.

The first step in developing a comprehensive fraud risk assessment is to communicate the steps

Table 4:

Step	Description
Establish risk assessment team	The risk assessment team should comprise expertise from across the Firm; this ensures maximum coverage with key understanding of operational eccentricities.
Determine starting point	Either target core areas of concern or establish a Firm-wide assessment.
Identify all relevant fraud schemes	Identify and assess risks at the entity, subsidiary, department, business line and functional levels.
Calculate score	This should take the form of a likelihood and impact assessment, calculated using the Firm's preferred methodology.
Control effectiveness and efficacy assessment	The risk assessment team should examine each specific risk, identify the existing related control, and evaluate efficacy in terms of mitigating fraud risk. If sufficient data exists, a review of effectiveness should also take place to ensure the limitation of later control failures.
Risk prioritisation	Firms should use the results of the likelihood and impact assessment to assess priority.
Document process	Key items to document could include the methodology used, assessment procedure, assessment results, response strategies, performing controls and operational weaknesses.

being taken and promote the process at all levels. The steps that could be undertaken are set out in Table 4.

The risk assessment should allow the Firm to create a risk map. It is up to Firm to develop how fraud risks are mapped to other risks and operations. However, it should align with the overall AFP and target maturity level, identifying the likely fraud schemes that the Firm is vulnerable to, both internally and externally, later integrating them into a more comprehensive risk map. Once a Firm is aware of the fraud risks faced, controls should be implemented where vulnerabilities have been identified.

At this stage, the Firm should have a control environment (eg, the standards, processes and structures) that forms the foundation for carrying out internal controls. It is prudent to point out that risk controls and compliance controls are nuanced but should be considered together. Whereas risk controls are methods that Firms use to assess potential loss and take action to reduce or eliminate identified risks, compliance controls can be categorised as interlocking activities driven by policies and procedures to ensure personnel act in line with the law and regulatory requirements. Compliance teams can be a vital source for communicating the AFP approach both internally and externally, communicating expectations and requirements internally while communicating the Firm's approach to regulators, externally.

Compliance and risk teams should work together to ensure control activities are developed and monitored. The activities undertaken by personnel, although a potential risk, can also be an excellent source of data, enabling a Firm to identify vulnerabilities and assess the efficacy of a control. As compliance controls are driven by policy and guidance, it is important that risk teams take part in developing guidelines that will generate appropriate data.

Whether basic or complex, data is critical to identifying fraud and implementing well-functioning controls to prevent it. However, any data is only as good as its component parts. Many systems available on the market can be highly intuitive, but if the data points being fed in to these systems are inaccurate, irrelevant or corrupt the results will be false (rubbish in, rubbish out). Larger Firms implementing these tools should assess the process driving datapoints on a regular basis.

Many anti-fraud tests can be easily implemented using basic spreadsheet software, at least initially. When collecting data to be used in the assessment of a control, the premise for small Firms remains the same as for large ones: assess the process driving datapoints on a regular basis.

It is notable that all information will not come from risk controls. As previously stated, personnel

Table 5:

Element	Description
Protocols	These are formal processes for receiving, evaluating and responding to reports of potential fraud. This also speaks to culture, ensuring personnel are aware and engaged. Communication should be clear, and training provided on how investigations are undertaken.
Reporting mechanism	This is generally determined by the governance structure. It may be appropriate to establish terms of reference, if a separate committee needs to be established in order to create independence of action.
Communication procedure	This should be a process for distributing the results of an investigation, within the governance structure in the first instance and more broadly to personnel through training, where appropriate.
Monitoring	Any action taken to correct the deficiency, however arising, should be documented and tracked to ensure gaps are closed having gone through sufficient oversight.
Investigation performance assessment	A broad assessment of the investigation should be conducted prior to its conclusion so that any unnecessary steps can be removed or additional steps added to the procedure to enhance the performance of future investigations. Some Firms conduct fire drills to assess investigatory performance.

are arguably one of a Firm's best monitoring tools. Information may come from self-reporting mechanisms (eg, whistleblower policy). Ensuring that there are robust anti-retaliatory provisions in internal reporting procedures will not only help embed the right culture but support the control environment.

The way in which a Firm makes use of information produced will be vital for monitoring, testing, oversight and any investigations that may be required.

RESPONSE

To respond to a potential fraud, whether through breach of policy, process, law or regulation, the Firm must have a mechanism to conduct thorough investigations to understand the root causes of fraud and how controls were either ineffective or not in place (FCA Principles for Businesses[11]).

Any response mechanism should be able to evaluate, communicate and remediate both potential fraud and the control deficiencies that lead to fraud. At a minimum, an investigations programme should have the elements set out in Table 5.

These elements describe the groundwork a Firm needs to have taken to be in a position to conduct an investigation. There are numerous considerations to take into account once an investigation is actually under way. Prior to starting any investigation, Firms should set a clearly defined scope of work with clear objectives that can be reflected in an investigation plan (can also be set out in terms of reference, if applicable). There is no one-size-fits-all solution. Table 6 sets out how the scope of an investigation will be affected.

In general, a typical investigation will include a series of steps that have additional considerations (see Table 7).

CONCLUSION

In conclusion, there is no one-size-fits-all approach to fraud prevention. This paper is not intended to be an exhaustive list of the steps Firms need to take in order to establish a framework – there are countless variations of individual components to frameworks, which would be too numerous to outline in a paper of this nature – but it provides a foundation for best practice.

If an investigation is opened, the implications of the outcome becoming reportable should be considered at each stage of the process. Investigation teams should be as independent as possible to allow for the investigation of senior management without undue pressure. Extensive audit trails of evidence gathering techniques, document review and resolution should be kept. Legal advice should be

Table 6:

Consideration	Description
Timing	This is key in circumstances where a self-report may have to be made. For example, the Serious Fraud Office (SFO) refers to 'within a reasonable time of the suspicions coming to light'.[12] This will probably allow for at least a preliminary investigation.
Confidentiality	The requirements of applicable data privacy rules (eg, GDPR[13]) must be considered.
Legal privilege	There is a risk that the internal investigation might result in the creation of nonprivileged documents, which could assist potential civil claims (by customers or shareholders).
Remediation	This could include potential self-reporting, disciplinary action against implicated personnel, or control implementation to ensure the conduct is not repeated.
Expert engagement	This speaks to the previous considerations, insofar as the investigating team may need access to legal counsel (external or internal), or the data protection officer. This will require that they are provided with the appropriate authority to act outside ordinary reporting lines.

Table 7:

Step	Consideration
Evidence gathering	Firms should establish categories of evidential materials (e-mails, electronic/hard-copy documents, external storage devices, mobile phones, tablets, internet messaging and chatroom data, telephone recordings[14]).
Data assessment	Investigation plans and procedures should help ensure the preservation of relevant data and document their consideration of the protection of 'data subjects'.
Compiling records	It is vital that the investigating team maintain an audit trail of evidence gathered and how it is being handled and the potential need for persons to provide witness statements.
Interviewing witnesses	The investigation team may wish to consider conducting 'informal interviews' initially to identify where evidence might be stored. All interviews should be approached with care (even those relating to the location of evidence) so as to avoid tainting the recollection of witnesses, particularly where there is a possibility of deciding to self-report upon conclusion of the investigation.
Final report	The default output should be the production of a factual summary. Notably, there is a risk it may not be privileged if the investigation finds that behaviour is criminal in nature and is reported.
Record keeping	Firms should keep clear records of key decisions taken, including the drafting of detailed, auditable summaries of data preservation techniques used in the collection and review process. It will also be important to preserve originals of all hard-copy documents and devices. The FCA Handbook states that where a Firm conducts an internal investigation, it will be 'very helpful' if the Firm maintains a proper record of the enquiries made and interviews conducted.[15]

obtained regarding employment law, legal privilege, and liability (where the timeline allows). It will also be important to maintain records of how the matter was resolved. All aspects of an investigation should remain confidential; communication to the wider business should involve how the control aspects were resolved (without disclosing specifics of an individual case) to ensure ongoing learning and awareness.

There will undoubtably be links and overlaps between frameworks. Any Firm should ensure that implementation of an AFP is taken as an opportunity to conduct a review of its entire risk ecosystem, streamlining other processes where necessary and addressing interconnected policies and processes. Firms may wish to assess maturity levels across their other frameworks by using the model outlined. The success or failure of any framework is

predicated on there being an embedded culture of accountability and understanding. When identifying gaps that cannot be managed by binary rule setting, Firms should set team-level authority processes, responsibility structures and granular accountability measures to ensure personnel are closely aligned with the outcomes.

References

1 'UK Finance 2021 Half-Year Fraud Update' p. 27, available at: https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf (accessed on 10th February, 2022)
2 'A Crackdown on Covid-19 Fraud Begins', available at: https://www.mazars.co.uk/Home/Services/Financial-advisory/Restructuring-and-Insolvency/Restructuring-Insolvency-Insights/A-crackdown-on-Covid-19-fraud-begins (accessed on 11th February, 2022)
3 The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, Financial Services (Electronic Money, Payment Services and Miscellaneous Amendments) (EU Exit) Regulations 2019, SI 2019/1212, available at: https://www.legislation.gov.uk/uksi/2019/1212/made (accessed on 11th February, 2022)
4 Financial Services and Markets Act 2000, section 2(B), available at: https://www.legislation.gov.uk/ukpga/2000/8/section/2B (accessed on 13th February, 2022)
5 Financial Conduct Authority Handbook Glossary, available at: https://www.handbook.fca.org.uk/handbook/glossary/G418.html (accessed on 13th February, 2022)
6 '2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.' p.30, available at: https://legacy.acfe.com/report-to-the-nations/2020/ (accessed on 14th February, 2022)
7 Fraud Act 2006, available at: www.cps.gov.uk/legal-guidance/fraud-act-2006 (accessed on 15th February, 2022)
8 'Financial Crime Guide: A Firm's Guide to Countering Financial Crime Risks', available at: https://www.handbook.fca.org.uk/handbook/FCG.pdf (accessed on 15th February, 2022)
9 FCA (2020) '"Messages from the Engine Room" 5 Conduct Questions: Industry Feedback for 2019/20 Wholesale Banking Supervision', available at: www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2019-20.pdf (accessed on 15th February, 2022)
10 *R (FCA) v Fabiana Abdel-Malek & Walid Choucair* [2020] EWCA Crim 1730.
11 'FCA Handbook' (PRIN 2.1.1R), available at: https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html (accessed on 15th February, 2022)
12 'SFO Operational Handbook, Corporate Co-operation Guidance, August 2019', available at: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/ (accessed on 16th February, 2022)
13 Council Regulation (EU) No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 16th February, 2022)
14 'FCA Handbook' (SYSC 10A.1), available at: https://www.handbook.fca.org.uk/handbook/SYSC/10A/1.html (accessed on 16th February, 2022)
15 'FCA Handbook' (EG 3.11.9), available at: https://www.handbook.fca.org.uk/handbook/EG/3/11.html (accessed on 16th February, 2022)