FINANCIAL CONDUCT AUTHORITY

Consultation Paper

CP24/9***

Financial Crime Guide Updates

April 2024

How to respond

We are asking for comments on this Consultation Paper (CP) by **27 June 2024**.

You can send them to us using the form on our website.

Or in writing to:

Financial Crime Policy,
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Telephone:
0207 066 0984

Email:
cp24-9@fca.org.uk

Sign up for our **news and publications alerts**

See all our latest press releases, consultations and speeches.

Disclaimer

When we make rules, we are required to publish:

- a list of the names of respondents who made representations where those respondents consented to the publication of their names,
- an account of the representations we receive, and
- an account of how we have responded to the representations.

In your response, please indicate:

- if you consent to the publication of your name. If you are replying from an organisation, we will assume that the respondent is the organisation and will publish that name, unless you indicate that you are responding in an individual capacity (in which case, we will publish your name),
- if you wish your response to be treated as confidential. We will have regard to this indication, but may not be able to maintain confidentiality where we are subject to a legal duty to publish or disclose the information in question.

We may be required to publish or disclose information, including confidential information, such as your name and the contents of your response if required to do so by law, for example under the Freedom of Information Act 2000, or in the discharge or our functions. Please note that we will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Irrespective of whether you indicate that your response should be treated as confidential, we are obliged to publish an account of all the representations we receive when we make the rules.

Further information on about the FCA's use of personal data can be found on the FCA website at: www.fca.org.uk/privacy.

Contents

Chapter 1

Summary

Why we are consulting

1.1 Financial crime – including fraud, money laundering, sanctions evasion, proliferation and terrorist financing – does enormous damage to society. It undermines market integrity and consumer confidence. Tackling financial crime requires a collective effort – from us, regulated firms, the Government, law enforcement and our regulatory partners. The national Economic Crime Plan 2 (2023 to 2026) and Fraud Strategy, both published by the Government in 2023, establish actions for public and private sector parties, with an ambition to reduce financial crime. Our work is part of this collective effort.

1.2 We are consulting on proposed changes to the FCA's Financial Crime Guide (The Guide). It's aim is to enhance understanding of our expectations and help firms assess the adequacy of their financial crime systems and controls and remedy deficiencies. It contains self-evaluation questions and examples of good and poor practice for firms drawn from FCA work and other financial crime publications.

1.3 Financial services firms should establish proportionate financial crime systems and controls, while serving their customers and markets. The Guide does not contain rules and imposes no new requirements on firms. We expect firms to have read and considered the Guide and to use their judgement on how it may help them to ensure they have effective policies and controls in place.

1.4 For further information on how these changes aim to prevent harm and how the consultation aligns with FCA objectives, see Chapters 2 & 3.

1.5 This CP should be read by:

- All FCA Financial Crime Supervised Firms.
- Firms that the FCA supervises under The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), including cryptoasset businesses.

1.6 The CP may also be of interest to:

- Individuals and organisations working with firms subject to FCA Financial Crime and MLRs supervision.
- Financial Services Sector Trade Associations.

1.7 Any other parties interested in FCA Financial Crime Supervision. This could include non-governmental organisations working on financial crime prevention or academics.

- This CP is targeted at firms and will be of limited relevance to consumers. Some consumers or consumer groups may also be interested in the Guide.

What we want to change

1.8 We want to ensure that the Guide remains clear, reflects our most relevant and recent findings, and supports firms in identifying and assessing that they have the right financial crime controls in place.

1.9 We propose changes to the following areas.

- **Sanctions:** Post Russia's illegal invasion of Ukraine in 2022, we conducted extensive assessments of firms' sanctions systems and controls. We propose to update this section to reflect what we and firms have learned.
- **Proliferation Financing (PF):** The guidance is being updated to ensure PF is explicitly referenced throughout the Guide where appropriate, and to highlight a 2022 update to the MLRs which requires firms to carry out PF Risk Assessments.
- **Transaction Monitoring:** We propose to set out some key guidance for firms on how they can implement and monitor transaction monitoring systems and support responsible innovation and new approaches, such as use of Artificial Intelligence.
- **Cryptoassets:** Cryptoasset businesses registered under the MLRs have been subject to FCA supervision for AML purposes since June 2020. We propose to make explicit reference that Cryptoasset businesses should consult the Guide.
- **Consumer Duty:** We propose that the Guide makes clear that firms should consider whether their systems and controls are proportionate and consistent with their obligations under the Duty.
- **Consequential Changes:** We are looking to make consequential changes to the Guide, including replacing expired links, outdated references to European Union rules and refreshed case studies drawing from more recent FCA enforcement notices.

1.10 Further details can be found in Chapters 2-3 and Annex A.

Outcomes and measuring success

1.11 We will evaluate the impact of the consultation by analysing the level of engagement and feedback on the proposed changes.

1.12 We will continue to update the guidance in line with our supervisory findings and publications. We also welcome feedback on chapters or areas not addressed in this CP on financial crime, that the industry considers we should focus on in future.

Next steps

1.13 As part of our ongoing ambition to make sure the Guide remains clear and supports firms, we will look to introduce through consultation further changes to the Guide as needed. This will likely include updates of the other chapters in the Guide, including those related to fraud.

1.14 Please send us your comments on the questions in this CP by 27/06/2024.

1.15 Use the online response form or write to us at the address provided.

1.16 We will consider your comments and plan to publish feedback on this CP, along with the final amended text of the Guide, in a Policy Statement. Your feedback will also instruct our future work updating the Guide.

Chapter 2

The wider context

2.1 Tackling financial crime is a priority for the FCA. As part of our responsibility to help ensure the integrity of the UK financial markets we require all authorised firms to have proportionate systems and controls in place to mitigate the risk that they might be used to commit financial crime.

2.2 Our strategy for 2022-2025 restates our commitment to reducing and preventing financial crime. This includes lowering incidences of money laundering through the firms we supervise directly. Financial crime harms society and the economy and erodes confidence in the UK financial system. We are seeking to help address these harms by updating the Guide.

Reducing financial crime

2.3 We are committed to making sure that firms and markets are not used as conduits for financial crime. These changes provide guidance to firms on actions they might take when evaluating or setting up their systems and controls.

Maintaining confidence in the financial system

2.4 The failure of firms to establish, implement and maintain adequate financial crime systems and controls exposes the financial system to financial crime. This can affect the reputation of individual firms, UK financial services and the UK as a whole. By providing guidance to help firms assess the adequacy of their systems and controls we are helping to mitigate this risk and encouraging confidence in the financial system.

Consumer protection

2.5 Good financial crime systems and controls can directly protect consumers and their money. Firms should have proportionate financial crime systems and controls, reflective of their business.

2.6 This will be reinforced by making it clear that all firms should also take into account whether their systems and controls are consistent with the Consumer Duty.

Chapter 3

Proposals for changes in the Financial Crime Guide

Sanctions

3.1 The unprecedented size, scale, and complexity of sanctions imposed by the UK Government and international partners since Russia's invasion of Ukraine, has further increased our focus on firms' sanctions systems and controls.

3.2 We have been engaged in a substantial programme of work assessing the systems and controls relating to sanctions compliance for over 170 firms across a range of sectors. This has involved assessing firms' controls, using a new analytics-based tool, as well as the use of specific intelligence and reporting.

3.3 We propose to make extensive updates to Chapter 7 covering Financial Sanctions. These updates will incorporate the key findings we published on 6 September 2023 as well as other supervisory findings. Our intention is not to refer to specific financial sanctions regimes currently in place, but to focus on the high-level systems and controls that allow firms we regulate to effectively meet their obligations. The proposals include:

- Reporting requirements that we have introduced for firms to report sanctions breaches or if a firm is directly or indirectly subject to any financial sanctions.
- Governance arrangements to oversee sanctions systems and controls. This includes senior management accountability, oversight of outsourced functions and engagement in public-private and private-private information/best practice sharing.
- Stressing the importance of management information to help ensure that the operation of sanctions systems controls is resourced and monitored effectively.
- While sanctions themselves are not risk-based, we have included further details on how firms consider their exposure to potential sanctions regimes and how they can prepare to respond to future sanctions measures in a timely manner.
- Providing more examples of our expectations and of good and poor practice when using screening tools to identify potential sanctions issues.
- Some specific guidance on the interplay between Customer Due Diligence (CDD)/ Know Your Customer (KYC) procedures for AML purposes and managing sanctions risks.
- New guidance on our expectations of how firms identify, assess and report potential sanctions breaches.

Proliferation financing

3.4 Since 2022 amendments to the MLRs have required firms to identify and assess the risks of proliferation financing to which its business is exposed. The changes are intended to update the guidance to reflect this requirement.

3.5 As set out in the Guide, firms need to understand their financial crime risks if they are to apply proportionate and effective systems and controls. Firms can decide whether they complete the risk assessment on PF as part of a wider risk assessment or as a standalone document. We propose to:

- Add references to PF Risk assessment in Chapter 7.2 'Risk Assessment' to reflect the requirement.
- Add links to useful material for firms to consult when conducting or reviewing their proliferation financing risk assessments.

Transaction monitoring

3.6 Transaction monitoring is a key control for almost all firms we regulate. In our supervisory work and support for innovation, we have seen examples of poor software deployment. Alongside this, we have also seen industry's desire to innovate using new technologies to improve the effectiveness of their systems to detect potential financial crime. Consequently, we are proposing to provide more guidance to help firms in adopting and maintaining automated monitoring systems. We intend to maintain our existing position that automated monitoring is only required where appropriate for the size and nature of the business and is not necessary if manual processes achieve an effective outcome. The specific guidance includes:

- New self-assessment questions and examples of good and poor practice clarifying our expectations for firms to ensure that triggers in automated systems are set in a way appropriate for the money laundering, terrorist financing and proliferation financing risks the firm faces.
- We propose good practice of controls around introducing switching from one automated monitoring system to another and our supervisory expectations that firms should use the information from transaction alerts to inform the risks of individual customers, and as part of their continuous monitoring of the efficacy of their overall control framework.
- Good and poor practice on evaluating the effectiveness of the monitoring system and understanding how it is set up.
- The importance of oversight, resource and expertise for effective screening in the form of examples of good and poor practice, and self-evaluation questions.

Cryptoassets

3.7 The FCA became the supervisor for certain cryptoasset businesses in January 2020. At the time we referenced the Guide as a source of useful material for these firms. Since

then, we have undertaken extensive work as part of our registration and supervisory activity to assess the suitability of how these firms are complying with their obligations under the MLRs.

3.8 Separately, in February 2023, the Government consulted on a future financial services' regulatory regime for cryptoassets. In October 2023, in the response to its consultation, the Government set out the expectation that once the cryptoasset regime is in place, firms undertaking regulated cryptoasset activities would likely need to adhere to the same financial crime standards and rules under the Financial Services and Markets Act that apply to equivalent or similar traditional financial services activities.

3.9 We propose to set an expectation that firms registered with us under the MLRs as cryptoasset businesses take into account the Guide when designing their financial crime systems and controls to comply with their obligations under the MLRs and UK Financial Sanctions regime. This will help these firms to prepare for demonstrating effective financial crime systems and controls when the future regime goes live. Recognising the evolving development of cryptoasset businesses and regulations, we will continue to seek to provide feedback on good and poor-quality applications under the MLRs and provide additional guidance for the new regime as it develops.

3.10 Since 1 September 2023, cryptoasset businesses in the UK are required to collect, verify and share information about cryptoasset transfers, known as the 'Travel Rule'. We propose to include reference to the travel rule in the section that already exists for customer payments, and we think the good and poor practice already in the Guide is likely to be as relevant to inter-cryptoasset transfers as they are for wire transfers.

3.11 We are also proposing some additions to the sections on risk assessment, handling higher risk situations and fraud, and to reflect some of the findings of good and poor practice when using blockchain analytics as part of transaction monitoring. In addition, we are proposing to provide links to useful guidance material for cryptoasset firms including guidance on compliance with the Travel Rule. We also propose to add an example of good practice in screening outbound transactions to identify cryptoassets wallet addresses linked to fraud.

Consumer Duty

3.12 On 31 July 2023, the FCA's Consumer Duty came into force for new and existing products and services that are open for sale or renewal. It comes into force on 31 July 2024 for closed products and services. Under the Duty firms must act to deliver good outcomes for retail customers. We are proposing to include text that reminds firms that, where relevant, the Duty must be considered alongside financial crime obligations. For further information on the Duty, see our guidance in FG22/5.

Consequential changes

3.13 We are proposing other changes which help to ensure the Guide remains up to date. These changes include:

- Refreshed links and more recent examples of outcomes on financial crime.
- Removal of references to European Union rules and supervisory authorities to ensure the regulatory references are consistent with changes following the UK's exit from the EU.
- Additional links to useful material for firms to consult when conducting or reviewing their systems and controls.
- Updated good and poor practice examples on data security.
- Other minor drafting changes as identified.

Question 1: **Do you agree with the suggested drafting as set out in this Consultation Paper?**

Question 2: **For future iterations of the Guide which chapters in the Guide would you like us to consult on or provide further guidance? Are there any financial crime topics currently not in the Guide that you would like us to consult on in the future?**

Question 3: **Do you foresee any unintended consequences from the proposals?**

Annex 1

Questions in this paper

Question 1: Do you agree with the suggested drafting as set out in this Consultation Paper?

Question 2: For future iterations of the Guide which chapters in the Guide would you like us to consult on or provide further guidance? Are there any financial crime topics currently not in the Guide that you would like us to consult on in the future?

Question 3: Do you foresee any unintended consequences from the proposals?

Question 4: Do you agree with our cost benefit analysis and conclusion? If you do not, please provide an explanation, including any estimated costs or benefits that may be relevant.

Question 5: Do you agree with the comments on the assessment of the equality and diversity considerations?

Annex 2

Cost benefit analysis

Introduction

1. FSMA, as amended by the Financial Services Act 2012, requires us to publish a cost benefit analysis (CBA) of our proposed rules. Specifically, section 138I requires us to publish a CBA of proposed rules, defined as 'an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made'.

2. This analysis presents estimates of the significant impacts of our proposal. We provide monetary values for the impacts where we believe it is reasonably practicable to do so. For others, we provide estimates of outcomes in other dimensions. Our proposals are based on carefully weighing up these multiple dimensions and reaching a judgement about the appropriate level of consumer protection, taking into account all the other impacts we foresee.

3. The CBA has the following structure:

- The Market
- Problem and rationale for intervention
- Our proposed intervention
- Baseline and key assumptions
- Benefits
- Costs
- Monitoring and evaluation.

The Market

4. Financial crime involves the misuse of financial services by criminals to obtain economic benefits. Financial crime creates significant damage to society, though undermining market integrity and reducing consumers' and market participants' confidence. The FCA aims to ensure that firms and markets are not used as conduits for financial crime, as part of our responsibility to ensure the integrity of the UK financial markets and to protect consumers from harm.

5. Financial crime is complex and can evolve rapidly, as criminals adopt technological innovations. Developments in recent years have required firms to increasingly adapt their monitoring and prevention on emerging risks of financial crime, such as sanctions monitoring, use of cryptoassets and proliferation financing among others.

Problem and rationale for intervention

6. Financial crime creates significant harmful side effects in financial markets and wider society. As a means of accessing the proceeds of crime, financial crime may facilitate activities such as fraud and drug trafficking, as well as corruption, sanctions evasion and terrorism. There is also direct harm to consumers from the crime facilitated by financial crime such as fraud, cybercrime and trafficking.

7. Financial crime facilitates illegal activities which cause direct harm to UK consumers. In addition to facilitating this direct harm, in economic terms, financial crime can also be considered a form of market failure called "externality", which can result in significant harm to consumers:

> **Externality:** Financial crime can be considered an externality and/or a misalignment of incentives. Parties to financial transactions may consider their own private costs and benefits, but not wider costs to society. Financial firms or employees that accept capital from potential money launderers may benefit financially from those transactions, but do not consider the risk that the transactions could fund illicit activity or motivate it further.

8. The rationale for intervention is to update the Guide to ensure that firms have the information on best practice so they can benchmark their systems and controls and keep them under review when there are internal or external changes to the risk.

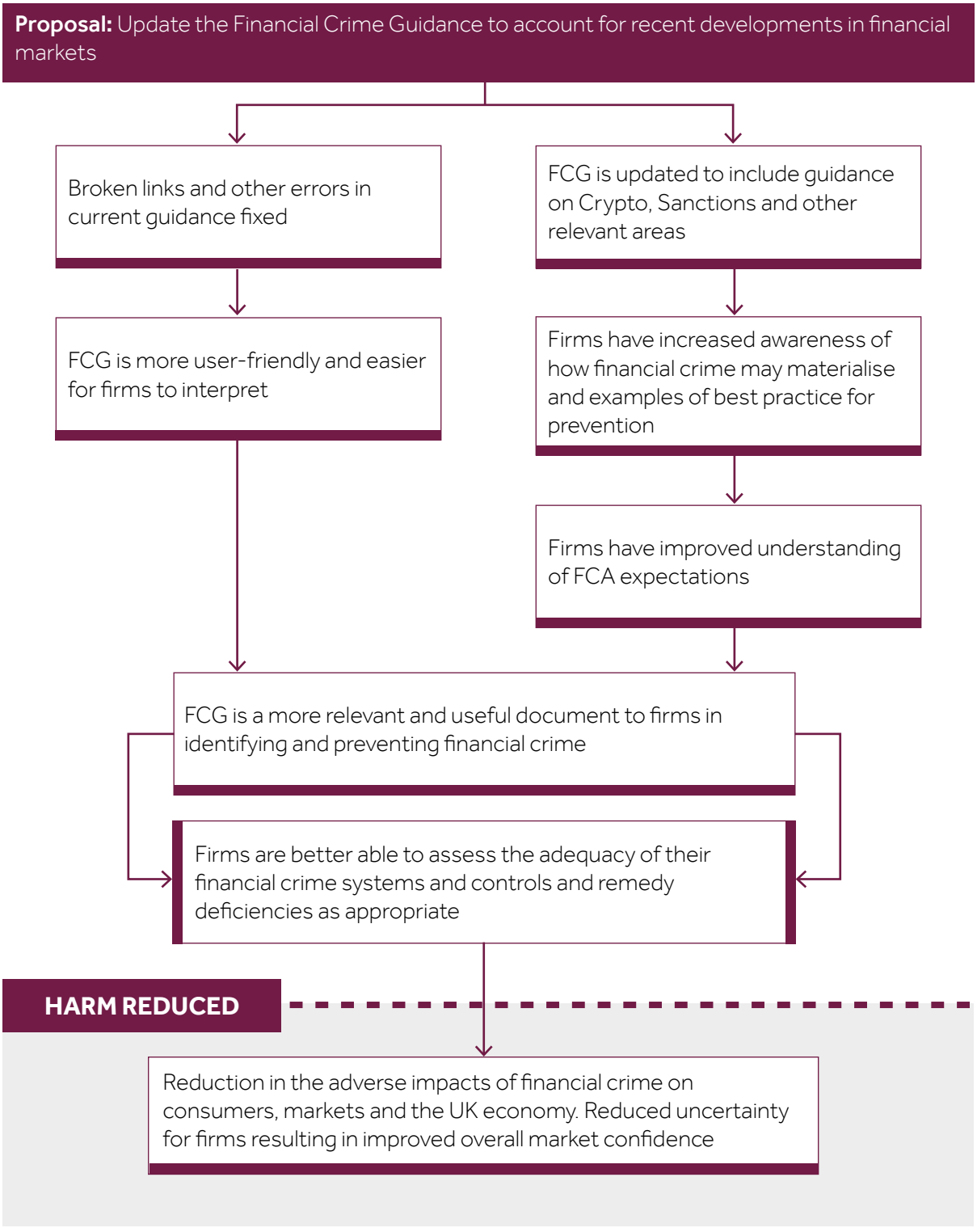
9. The intervention is also sought, due to potential future risk of lack of guidance and having outdated documents used by firms in assistance for their evaluation of financial crime systems and controls. Having inadequate controls increases the risk of financial crime, which may reduce market integrity and could result in significant consumer harm.

Our proposed intervention

10. We are proposing several changes to the current Guide in order to make it more useful to firms we regulate. We want to ensure the FCG remains an effective tool in supporting firms to identify and assess financial crime controls that are relevant to them. Our proposal is to update the FCG in specific areas, as outlined in the CP. These changes will primarily involve:

- **Quality of Life improvements:** This will involve updating expired links, refreshing references, and changes for clarity.
- **Additional guidance on novel areas of financial crime:** Including guidance on cryptoassets, sanctions, transaction monitoring and proliferation financing. This will ensure that the Guide remains up-to-date and relevant to firms in applying and interpreting our financial crime publications.

11. Through updating the FCG, we expect firms to be better placed to monitor and understand financial crime risks, identify any weaknesses in their current systems and controls and through this, reduce instances of financial crime. This is outlined in our causal chain below.



Baseline and key assumptions

12. It is necessary to establish a baseline against which to assess the costs and benefits of an intervention to ensure that only those attributable to the intervention are considered.

13. Our counterfactual scenario is that, without an intervention, the FCG would not be updated and could become less effective in helping regulated firms to identify and prevent financial crime.

14. Firms would not face any additional costs beyond those they already face.

15. In our analysis, the estimates of one-off and ongoing costs are based on our standardised cost model in which costs depend on a firm's size. The model differentiates between large, medium and small firms, basing this classification using data on firms' annual FCA fee blocks, and ranking them accordingly. We define the highest ranking 250 firms as large, the next highest ranking 1,500 firms as medium, and all remaining firms as small. We report average cost estimates. As these figures are mean averages, individual firms may experience higher or lower costs than those set out below.

16. We assume that the primary costs to firms from our intervention will be one-off familiarisation costs associated with considering and reading the CP and the updated Guide. This assumption is consistent with our view that firms are already following the practices set out in the guidance and will not require changes to business models.

17. We assume the number of compliance staff required to review changes to the FCG will be small. This is equivalent to:

- 6 staff per large firm,
- 4 per medium firm
- 1 per small firm.

18. We assume 13 pages of consultation paper and 26 pages of additional text will be required to be reviewed. We assume a GAP analysis will not be required by firms.

19. However, in addition to familiarisation costs, we assume that a limited number of firms will undertake a small change project and gap analysis in order to update their business models and account for the new guidance. We do not have data on the number of firms that would be required to undertake a change project, although as noted above, we believe most firms are already compliant with the practices the updated FCG will set out. We assume this additional cost will affect 5% of regulated firms (spread uniformly across small, medium and large). This assumption is based on our estimate of the number of firms that will undertake significant change projects as a result of the updated Guide.

20. We assume these firms will need to undertake a "Very Small" change project, requiring board approval. In terms of total person days for project team and manager, this assumption is equivalent to:

- 45 person days per large firm
- 14 person days per medium firm
- 3 person days per small firm.

21. We assume that the guidance will impact all firms regulated by the FCA. This gives us a firm population of ~45,000.

Benefits

22. The primary benefits associated with our intervention is reduced instances of financial crime, which would result in increased consumer confidence and market integrity. Certain firms may also experience increased efficiencies as a result of proposals. For example, updating broken links in the FCG could allow firms using the guidance to reduce the amount of time they spend on interpreting the FCG and ensuring they are following our recommended approach. We have not attempted to quantify these benefits.

Costs

23. In this section we outline our estimates of the costs for firms due to our proposed intervention. We use standardised assumptions to estimate firm compliance costs. Further details about our approach can be found in the publication "How we analyse the costs and benefits of our policies".

24. As noted above, we consider costs incurred to firms as a result of the proposed intervention to be small, one-off and limited to familiarisation costs. These costs take account of the time and resources that would have to be spent by firms to familiarise themselves with the proposals. Using the Standardised Cost Model, we estimate the one-off costs familiarisation to the industry to be around £10m.

25. For individual firms total cost varies conditional upon whether a firm needs to undertake a change project to align with the updated FCG. For firms which do not, we estimate familiarisation costs at £720 per large firm, £450 per medium firm and £140 per small firm. These numbers are rounded averages and individual firms may experience higher or lower costs than those set out here.

26. For firms which do undertake a change project (estimated 5% of total firms) we expect costs to be higher. We estimate total costs to these firms of £19,250 per large firm, £6,000 for a medium firm and £1,100 for a small firm. As above, these numbers are rounded averages and individual firms may experience higher or lower costs than those set out here.

Estimated implementation costs (aggregate across firm types)

	Large Firm	Medium Firm	Small Firm	Total
Familiarisation and gap analysis	£0.2m	£0.7m	£6.3m	£7.2m
Training	-	-	-	-
IT project	-	-	-	-

	Large Firm	Medium Firm	Small Firm	Total
Change project	£0.2m	£0.4m	£2.1m	£2.8m
Sales, customer, or other changes	-	-	-	-
Total costs	£0.4m	£1.1m	£8.4m	£10m

Numbers may not sum due to rounding

Estimated implementation costs (by firm types, for firms which will not need to undertake change project)

	Large Firm	Medium Firm	Small Firm	Average
Familiarisation and gap analysis	£720	£450	£140	£170
Training	-	-	-	-
IT project	-	-	-	-
Change project	-	-	-	-
Sales, customer, or other changes	-	-	-	-
Total costs	£810	£510	£150	£170

Numbers may not sum due to rounding

Estimated implementation costs (by firm types, for firms which will be required to undertake change project (assumed 5%))

	Large Firm	Medium Firm	Small Firm	Average
Familiarisation and gap analysis	£720	£450	£140	£150
Training	-	-	-	-
IT project	-	-	-	-
Change project	£18,500	£5,600	£950	£1,200
Sales, customer, or other changes	-	-	-	-
Total costs	£19,250	£6,000	£1,100	£1,350

Numbers may not sum due to rounding

27. As highlighted above, while individual costs are expected to be small, the total costs are driven by the population of firms we expect to be affected by changes to the FCG (i.e., all firms). We consider these costs proportionate to the expected benefits of our intervention (reduced financial crime).

28. Costs for firms which will be required to undertake a change project to align their business practices are significantly higher relative to firms which will only undertake familiarisation costs. However, given the significant costs of financial crime, we believe these additional costs are proportionate to the benefits associated with updating the Guide.

Monitoring and evaluation

29. We will evaluate the impact of the consultation through analysis of the level of engagement, and feedback on the proposed changes in this consultation. We will also continue to engage with firms to understand how they are using the FCG and whether additional updates are required in the future.

Question 4: **Do you agree with our cost benefit analysis and conclusion? If you do not, please provide an explanation, including any estimated costs or benefits that may be relevant.**

Annex 3

Compatibility statement

Compliance with legal requirements

1. This consultation does not propose the making of rules under the Financial Services and Markets Act 2000 (FSMA). As such, it is not subject to rulemaking requirements. It does, however, propose changes to FCA guidance and aligns with FCA's strategic objective of ensuring that markets function well and advances its operational objectives of integrity and consumer protection.

2. The proposed rules are compatible with the duty on the FCA to discharge its general functions (which include rulemaking) in a way which promotes effective competition in the interests of consumers (s. 1B (4)). The consultation is compatible with our integrity objectives by ensuring our financial crime supervisory population takes account of the Guide and have compliant systems and controls.

3. This consultation has taken into account the letter from the Chancellor of the Exchequer to the Chief Executive of the Financial Conduct Authority (FCA) providing recommendations for the FCA. This consultation is compatible with our operational objective to protect and enhance the integrity of the UK financial system. It is also aligned with the Government's economic policy strategic objective of maintaining a resilient, effectively regulated, and internationally competitive financial system that supports the economy, while protecting consumers and safeguarding taxpayer interests.

The FCA's objectives and regulatory principles: Compatibility statement

4. The proposals set out in this consultation are primarily intended to advance the FCA's operational objective of ensuring that the relevant markets function well. Changes are also relevant to the FCA's integrity and consumer protection objectives.

5. We consider these proposals are compatible with the FCA's strategic objective of ensuring that the relevant markets function well, through reducing and preventing financial crime. The consultation aligns with our objective to publish findings from our reviews and provide feedback to industry on what we see, so firms can improve their controls.

6. We are confident that the new guidance is compatible with our secondary international competitiveness and growth objective. Financial crime harms consumer confidence in the UK's financial sector and its reputation internationally. The guidance set out in this CP helps to ensure that firms can be confident they are fulfilling their obligations with regards to AML, Counter Terrorist Financing (CTF), sanctions and PF, while also allowing

firms to take an innovative, technology-led approach if they wish. Firms that utilise innovative solutions will be able to reinvest their efficiency savings in productive areas of their businesses, facilitating economic growth.

7. In preparing the proposals set out in this consultation, the FCA has had regard to the regulatory principles set out in s. 3B FSMA of:

The need to use our resources in the most efficient and economical way

8. Publishing our regulatory findings and providing feedback and communication to the industry on financial crime systems and controls is a cost-effective way of using our resources. FCA applies a risk-based approach to supervision, targeting more of our resource to where risk is greater and deploying a range of tools, including providing guidance to firms. With guidance we can communicate, in addition to other publications, our supervisory findings, including on those firms at higher risk.

The principle that a burden or restriction should be proportionate to the benefits

9. As set out in the CBA, we do not consider these changes to place a disproportionate burden or restrictions on firms. The provisions provide more clarity from which firms can benefit. The Financial Crime Guide provides guidance and firms can decide how they use it on a risk-based approach.

The general principle that consumers should take responsibility for their decisions

10. The consultation is not aimed as guidance for the consumer and thus will have limited consumer impact. However, through better financial crime controls at firms that consumers use, we believe that the financial crime guide and better guidance will result indirectly in better consumer outcomes and protection.

The responsibilities of senior management

11. The consultation does not propose changes to the responsibilities of senior management.

The desirability of recognising differences in the nature of, and objectives of, businesses carried on by different persons including mutual societies and other kinds of business organisation

12. The consultation is proposing changes as guidance only. A business can have regard to the guidance as it sees fit.

The desirability of publishing information relating to persons subject to requirements imposed under FSMA, or requiring them to publish information

13. This consultation is aligned with this objective. It is providing further information to firms subject to FSMA Financial Crime Rules.

The principle that we should exercise our functions as transparently as possible

14. The consultation is aligned with this objective and provides transparent communication on our proposals to the firms we supervise.

15. In formulating these proposals, the FCA is taking regard of the importance of taking action intended to minimise the extent to which it is possible for a business carried on (i) by an authorised person or a recognised investment exchange; or (ii) in contravention of the general prohibition, to be used for a purpose connected with financial crime (as required by s. 1B(5)(b) FSMA).

Legislative and Regulatory Reform Act 2006 (LRRA)

16. We have had regard to the principles in the LRRA when preparing these proposals for the parts of the proposals that consist of general policies, principles or guidance.

17. These principles are that regulatory activities should be carried out in a way which is:

- transparent
- accountable
- proportionate
- consistent and
- targeted only at cases in which action is needed.

18. The proposals in the CP are aimed to help ensure effective compliance in the firms we supervise. By publishing good and poor practice and our supervisory findings in the financial crime guide, we are providing firms with more detailed guidance on our expectations and the outcomes we want to see. We note that the Guide is for guidance only and firms should use a risk-based approach. There are no rule changes, the proposals are proportionate and aimed at assisting the supervised firms.

19. We have also had regard to the supplementary principles of the Regulators' Code that:

- Regulators should carry out their activities in a way that supports those they regulate to comply and grow;
- Regulators should provide simple and straightforward ways to engage with those they regulate and hear their views;
- Regulators should base their regulatory activities on risk;
- Regulators should share information with each other about compliance and risk

- Regulators should ensure clear information, guidance and advice is available to help those they regulate meet their responsibilities to comply and;
- Regulators should ensure that their approach to their regulatory activities is transparent.

20. We consider that our proposals support firms by providing clear guidance about how they can meet or benchmark their controls on financial crime in an effective, risk-based and proportionate way.

Expected effect on mutual societies

21. The FCA does not expect the proposals in this paper to have a significant impact on mutual societies.

22. Some mutual societies are excluded under the Money Laundering Regulations, Regulation 15.

Equality and diversity considerations

23. We have considered the equality and diversity issues that may arise from these and concluded that they do not materially impact any of the groups with protected characteristics under the Equality Act 2010. But we will continue to consider the equality and diversity implications of the proposals during the consultation period and will revisit them when finalising our guidance.

24. In the meantime, we welcome input to the consultation on this.

Question 5: **Do you agree with the comments on the assessment of the equality and diversity considerations?**

Annex 4

Abbreviations in this document

Abbreviation	Description
AML	Anti-Money Laundering
CBA	Cost Benefit Analysis
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FSA	Financial Services Authority (predecessor to FCA)
FSMA	Financial Services and Markets Act 2000
FCG	Financial Crime Guide
KYC	Know Your Customer
MLRs	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
MLRs 2022	The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022
OFSI	The Office of Financial Sanctions Implementation
PF	Proliferation Financing
TM	Transaction Monitoring

All our publications are available to download from www.fca.org.uk.

Request an alternative format

Please complete this form if you require this content in an alternative format.

Or call 020 7066 6087

Sign up for our **news and publications alerts**

Appendix 1

Draft Handbook text

FINANCIAL CRIME GUIDE (AMENDMENT) INSTRUMENT 2024

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the powers and related provisions in or under:

(1) section 139A (Power of the FCA to give guidance) of the Financial Services and Markets Act 2000;
(2) regulation 120(1) (Guidance) of the Payment Services Regulations 2017; and
(3) regulation 60(1) (Guidance) of the Electronic Money Regulations 2011.

Commencement

B. This instrument comes into force on [*date*].

Amendments to material outside the Handbook

C. The Financial Crime Guide: A firm's guide to countering financial crime risks (FCG) is amended in accordance with the Annex to this instrument.

Citation

D. This instrument may be cited as the Financial Crime Guide (Amendment) Instrument 2024.

By order of the Board
[*date*]

Annex

Amendments to the Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)

In this Annex, underlining indicates new text and striking through indicates deleted text.

1 Introduction

1.1 What is the FCG?

…

1.1.5 The material in *FCG* does not form part of the *Handbook*, but it does contain *guidance* on *Handbook rules* and *principles*, particularly:

…

Where *FCG* refers to guidance in relation to *SYSC* requirements, this may also be relevant to compliance with the corresponding Principle in our Principles for Businesses and corresponding requirements in the *Payment Services Regulations* and the *Electronic Money Regulations*. All elements of the *FCG* but particularly *FCG* 3 on money laundering and *FCG* 7 on sanctions will be relevant to cryptoasset businesses registered with us under the *Money Laundering Regulations*.

…

1.1.11 *FCG* is not a standalone document; it does not attempt to set out all applicable requirements and should be read in conjunction with existing laws, rules and guidance on financial crime. If there is a discrepancy between *FCG* and any applicable legal requirements, the provisions of the relevant requirement prevail. If firms have any doubt about a legal or other provision or their responsibilities under FSMA or other relevant legislation or requirements, they should seek appropriate professional advice.

Among other requirements, firms should consider whether their financial crime systems and controls are consistent with their obligations, if any, under the Consumer Duty. For instance, in complying with the Duty, firms may wish to consider additional steps in their customer journeys to help prevent fraud. They may also consider offering additional consumer support, such as:

- a real-time human interface to deal with security or fraud concerns;
- engagement with customers during customer due diligence processes; or
- providing information on their application or application outcome for products and services.

…

3 Money laundering and terrorist financing

…

3.2 Themes

…

The Money Laundering Reporting Officer (MLRO)

3.2.2 …

Firms to which this section applies must appoint an individual as MLRO. The MLRO is responsible for oversight of the firm's compliance with its anti-money laundering obligations and should act as a focal point for the firm's AML activity. Regulation 21(1)(a) of the *Money Laundering Regulations* also requires the appointment of a senior manager as the officer responsible for the relevant person's compliance with these regulations. Where appropriate, this section can be relevant for how that person meets their obligations under the *Money Laundering Regulations*.

…

Risk assessment

3.2.3 The guidance in *FCG* 2.2.4G and *FCG* 7.2.5G on risk assessment in relation to financial crime and proliferation financing also applies ~~to AML~~.

The assessment of ~~money laundering~~ financial crime and proliferation financing risk is at the core of the firm's AML/CTF/PF effort and is essential to the development of effective AML/CTF/PF policies and procedures. A firm is required by Regulation 18 of the *Money Laundering Regulations* to undertake a risk assessment. This also includes a risk assessment by relevant persons in relation to proliferation financing as set out in Regulation 18A.

Firms must therefore put in place systems and controls to identify, assess, monitor and manage money laundering, terrorist financing and proliferation financing risk. These systems and controls must be comprehensive and proportionate to the nature, scale and complexity of a firm's activities. Firms must regularly review their risk assessment to ensure it remains current.

Self-assessment questions:

- Which parts of the business present **greater risks** of money laundering, terrorist and proliferation financing? (Has your firm identified the risks associated with different types of ~~customer~~ customers or beneficial ~~owner, product~~ owners, products, services, activities, transactions, business ~~line~~ lines, geographical ~~location~~ locations and delivery ~~channel~~ channels (e.g. internet, telephone, branches)? Has it assessed the extent to which these risks are likely to be an issue for the firm?)
- How does the risk assessment inform your day-to-day operations? (For example, is there evidence that it informs the level of customer due diligence you apply or your decisions about accepting or maintaining relationships?)

- For cryptoasset businesses, how are the risks of different types of cryptoasset (e.g. anonymity-enhanced or privacy coins) or wallet solutions and addresses assessed?

Examples of good practice	Examples of poor practice
…	
• The firm has identified good sources of information on money laundering, terrorist financing and proliferation financing risks, such as National Risk Assessments, ~~ESA Guidelines,~~ FATF mutual evaluations and typology reports, NCA alerts, press reports, court judgements, reports by non-governmental organisations and commercial due diligence providers.	• Higher risk countries are allocated low-risk scores to avoid enhanced due diligence measures.
• Consideration of money laundering, terrorist financing and proliferation financing risk associated with individual business relationships takes account of factors such as: o company structures; o political connections; o country risk; o the customer's or beneficial owner's reputation; o source of wealth; o source of funds; o expected account activity; o factors relating to its customer's countries or geographic areas of operations; o products and services; o transactions; o delivery channels; o sector risk; and o involvement in public contracts.	• Relationship managers are able to **override customer risk scores** without sufficient evidence to support their decision.
…	

…

Customer due diligence (CDD) checks

3.2.4 …

Self-assessment questions:

- …
- Are procedures **sufficiently flexible** to cope with customers who cannot provide more common forms of identification (ID)?
- With **non-face-to-face** transactions, how does the firm's approach provide confidence that the person is **who they claim to be**? How is any technology used as part of onboarding tested?

…

Ongoing monitoring

3.2.5 …

Self-assessment questions:

…

- How do you feed the **findings from monitoring** back into the customer's risk profile?
- Do you frequently **review** the monitoring system rules and typologies for effectiveness? Do you **understand** the threshold and rule rationales?

Examples of good practice	Examples of poor practice
…	
• The firm uses **monitoring results** to review whether CDD remains adequate.	• A cryptoasset business assumes that blockchain analysis is all that is required to monitor transactions and fails to do its **own transaction monitoring** based on the **knowledge** of its customers or **relying on** off-chain information.
• The firm takes advantage of **customer contact** as an opportunity to update due diligence information.	• The firm's measures fail to conduct **full assessment** of the risk. For instance, the firm does not consider **changes** in the nature of the relationship or expected activities.
• The firm demonstrates a **risk-based approach** following a **monitoring event**. This could include implementing regular periodic	

reviews and having procedures for event-driven reviews.	
…	

See regulations 27, 28(11), 33, 34 of the *Money Laundering Regulations*.

The use of transaction monitoring

3.2.5A This section is relevant to a firm using transaction monitoring as part of its ongoing monitoring efforts to detect money laundering, financing of terrorism and proliferation financing (see 'ongoing monitoring' in *FCG* 3.2.5G). This could be relevant to firms serving either retail or wholesale customers.

To date, many large institutions have used transaction monitoring systems that work on a transaction-by-transaction basis, flagging fund movements that exceed rule-driven thresholds for human scrutiny. We understand that more sophisticated approaches show potential in this area, are able to take a more rounded view of customer behaviour, and, for example, show how the customer fits into broader networks of activity. Examples of such sophisticated technologies include the use of machine learning tools or artificial intelligence (AI) based tools to detect suspicious activity, or to triage existing alerts.

Self-assessment questions:

- Do you have an **understanding of the effectiveness** of your automated monitoring in different business lines?
- What actions have been taken to **mitigate shortcomings** that have been identified in business lines?
- What **consideration** has been given to alternative varieties of automated monitoring, including the use of novel approaches?
- Where a firm uses automated methods for **triaging alerts** generated by threshold-driven transaction-monitoring systems (e.g. scorecards overlaid on existing systems, 'hibernation' of alerts until further data prompts it to be revisited, or other systems to prioritise which alerts receive manual attention), can this be **justified** within the context of the firm's overall approach to monitoring?

Examples of good practice	Examples of poor practice
• New approaches are piloted or subject to evaluation periods, with firms able to demonstrate **appropriate testing**.	
• Monitoring arrangements (whether automated or manual or both) seek to take a **holistic view** of customer	• The **control framework** around automated monitoring is **weak**. For example, senior management have

behaviour and draw on a range of data, rather than just transaction-by-transaction analysis.	an unrealistic expectation of what automated monitoring systems are feasibly able to achieve, while manual scrutiny of alerts lacks resources and is unable to cope.
• Monitoring is applied, where appropriate, at multiple levels of aggregation: ○ transaction level (the lowest); ○ account level (the aggregate of transactions for an account); ○ customer level (the aggregate of accounts for a specific customer); and ○ linked-entity level (i.e. across a group of linked customers by relationship managers).	• Threshold-based transaction monitoring **approaches** are used in situations where they are **not suitable**, while other methods of scrutiny (such as oversight of customers by relationship managers) are neglected.
• When **decommissioning** an existing automated system (or aspects of that system, such as particular rule sets), a firm is able to **justify** this decision. Consideration may be given to, for example, the relative merits of other approaches (including manual approaches), the systems' resource implications, and the systems' performance outcomes (such as the intelligence-value of alerts and the proportion of 'false positives').	• A threshold-based, rule-driven transaction monitoring system is used, but is **poorly calibrated**, and the firm **struggles to articulate the rationale** for particular rules and scenarios.
• Before a new system replaces an existing one, a **robust judgement** is formed about the relative **usefulness of both systems.** While each system may not flag all the same events, the firm is able to demonstrate that one approach produces better-quality alerts overall.	• Data feeds fed into an automated system are not migrated smoothly when feeder systems are modified or upgraded or transactions from a specific system have been erroneously omitted from the transaction monitoring system.
• A firm **explores** the use of **new approaches** to automated monitoring (e.g. network analysis or machine learning). Consideration is given to the **limitations** of these approaches, and how any resultant	

risks can be contained. (For example, it will not be clear to operators of more free-form varieties of machine learning why the software has made its recommendations, which can pose ethical and audit challenges.)	
• The firm **tailors** the monitoring system rules to its **business**, **risk and relevant typologies**. The system and rules are **tested and reviewed** for right outcomes	• The firm uses a transaction monitoring system with set rules (which could include use of off-the-shelf systems) and does **not calibrate** these to the **firms' individual needs** or **review** them regularly for efficiency.
• The firm practices **good record keeping**. For example, records of decision making and rationales for thresholds are documented and accessible.	
• Where a firm learns that criminals have abused its facilities, a **review** is performed to **learn** how monitoring methods could be improved to **lessen the risk of recurrence**.	
	• A firm **does not verify** that a **counterparty** firm is monitoring customer activity.
	• A firm using an automated system **lacks an understanding of what the system is detecting and why**. This may be because of, for example, staff turnover, poor documentation or weak communication with the system's vendor.

See regulations 27, 28(11), 33, 34 of the *Money Laundering Regulations*.

Case study – transaction monitoring

3.2.5B The *FCA* found that 3 key parts of bank's transaction monitoring systems showed serious weaknesses over an extended period, measured in years. The systems

were ineffective and not sufficiently risk sensitive for a prolonged period. They exposed the bank and community to avoidable risks.

In particular, the bank failed to:

- consider whether the scenarios used to identify indicators of money laundering or terrorist financing covered relevant risks;
- carry out timely risk assessments for new scenarios;
- appropriately test and update the parameters within the systems that were used to determine whether a transaction was indicative of potentially suspicious activity. There was a failure to understand those rules and certain thresholds set made it almost impossible for the relevant scenarios to identify potentially suspicious activity; and
- check the accuracy and completeness of the data being fed into, and contained within, monitoring systems. This resulted in millions of transactions worth billions of pounds that were either monitored incorrectly or not at all.

The *FCA* imposed a financial penalty on the bank.

Handling higher risk situations

3.2.7 …

The *Money Laundering Regulations* also set out some scenarios in which specific enhanced due diligence measures have to be applied:

- **Correspondent relationships**: where a correspondent credit institution or financial institution, involving the execution of payment, is ~~outside the EEA~~ from a third country (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 34), the UK credit or financial institution should apply both EDD measures in Regulation 33 as well as additional measures outlined in Regulation 34 commensurate to the risk of the relationship. This can include in higher risk situations thoroughly understanding its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must also give approval before establishing a new correspondent relationship. JMLSG guidance sets out how firms should apply EDD in differing correspondent trading relationships.

…

- **Business relationships or a 'relevant transaction' where either party is established in a high risk third country**: the *Money Laundering Regulations* defines:

  (a) a high-risk third country ~~as being one identified by the EU Commission by a delegated act. See EU Regulation 2016/1675 (as amended from time to time);~~ is defined for the purposes of the MLRs as a country named by FATF on its list of High-Risk Jurisdictions

subject to a Call for Action or Jurisdictions under Increased Monitoring;

…

- **Other transactions**: EDD must be performed:

  …

  (b) in any other case which by its nature can present a higher risk of money laundering, proliferation financing or terrorist financing. This can include where there is evidence that a cryptoasset transaction has involved privacy-enhancing techniques or products such as 'mixers' or 'tumblers', privacy coins and transactions involving the use of self-hosted addresses, obfuscated ledger technology, ring signatures, stealth addresses, ring confidential transactions, atomic swaps and non-interactive zero knowledge proofs; and

  (c) where findings from blockchain analysis indicated exposure to criminal or sanctioned activities.

…

…

Customer payments

3.2.13 This section applies to banks subject to *SYSC* 6.3.

Interbank payments can be abused by criminals. International policymakers have taken steps intended to increase the transparency of interbank payments, allowing law enforcement agencies to more easily trace payments related to, for example, drug trafficking or terrorism. ~~The Funds Transfer Regulation~~ The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 requires banks to collect and attach information about payers and payees of wire transfers (such as names and addresses~~, or, if a payment moves within the EU, a unique identifier like an account number~~) to payment messages. Banks are also required to check this information is present on inbound payments, and chase missing data. The *FCA* has a legal responsibility to supervise banks' compliance with these requirements. Concerns have also been raised about interbank transfers known as "cover payments" (see *FCG* Annex 1) that can be abused to disguise funds' origins. To address these concerns, the SWIFT payment messaging system now allows originator and beneficiary information to accompany these payments.

From 1 September 2023, similar obligations have applied for cryptoasset transfers undertaken by cryptoasset businesses registered with the *FCA* under the *Money Laundering Regulations*. This chapter may assist cryptoasset businesses in implementing this requirement but they should also have regard to specific expectations set out by the *FCA*. See https://www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule.

Self-assessment questions:

- …
- ~~Does the firm use guidance issued by the ESAs? [**Editor's Note**: see http://www.eba.europa.eu/-/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers.].~~

…

Case study – poor AML controls

3.2.14 …

See the ~~*FSA's*~~ *FCA's* press release for more information: ~~www.fsa.gov.uk/pages/Library/Communication/PR/2010/077.shtml~~ https://www.fca.org.uk/publication/final-notices/alpari.pdf

…

Case study – poor AML controls: PEPs and high-risk customers

3.2.16 …

~~This was the largest fine yet levied by the *FSA* for failures related to financial crime~~.

See the ~~*FSA's*~~ *FCA's* press release for more information: ~~www.fsa.gov.uk/library/communication/pr/2012/032.shtml~~ https://www.fca.org.uk/publication/final-notices/coutts-mar12.pdf

Poor AML controls: risk assessment

3.2.17 …

See the ~~*FSA's*~~ *FCA's* press release for more information: ~~www.fsa.gov.uk/library/communication/pr/2012/055.shtml~~ https://www.fca.org.uk/publication/final-notices/habib-bank.pdf

…

3.4 Sources of further information

3.4.1 To find out more on **anti-money laundering**, see:

- …
- The UK National risk assessment of money laundering and terrorist financing ~~2017~~ 2020 - ~~https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017~~ https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020
- …

3.4.2 To find out more on countering terrorist finance, see:

- …
- ~~The European Supervisory Authorities (ESAs) have published risk factors guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849- https://www.eba.europa.eu/-/esas-publish-aml-cft-guidelines~~
- …

3.4.3 To find out more on customer payments, see:

- …
- The Wolfsberg Group's statement on payment standards: ~~**https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf**~~ https://db.wolfsberg-group.org/assets/373dbb28-b518-4080-82cc-4be7a54aa16e/Wolfsberg%20Group%20Payment%20Transparency%20Standards%202023.pdf
- ~~Joint Guidelines to prevent terrorist financing and money laundering in electronic fund transfers- http://www.eba.europa.eu/-/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers~~
- ~~The Funds Transfer Regulation (EU Regulation 847/2015 on information on the payer accompanying transfers of funds): http://data.europa.eu/eli/reg/2015/847/oj~~
- The Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017: https://www.legislation.gov.uk/uksi/2017/692/contents/made
- For cryptoasset businesses, see Annex I to Chapter 22 of Part II (Cryptoassets Transfers (Travel Rule)) JMLSG: www.jmlsg.org.uk
- *FCA* statement: https://www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule

3.4.4 …

3.4.5 To find out more on proliferation financing, see:

- The UK National risk assessment of proliferation financing 2021: https://assets.publishing.service.gov.uk/media/65a01397e96df50014f844fe/Risk_assessment_of_proliferation_financing__1_.pdf
- FATF work on proliferation financing: https://www.fatf-gafi.org/en/topics/proliferation-financing.html

4 Fraud

…

4.2 Themes

Preventing losses from fraud

4.2.1 …

Examples of good practice	Examples of poor practice
…	
• **Enhanced due diligence** is performed on higher risk customers (e.g. commercial customers with limited financial history. See 'long firm fraud' in *FCG* Annex 1).	• **Remuneration structures** may incentivise behaviour that increases the risk of mortgage fraud.
• Cryptoasset businesses **pre-screen** outbound transactions for addresses **linked to fraud**.	

…

Enforcement action against mortgage brokers

4.2.4 ~~Since the *FSA* began regulating mortgage brokers in October 2004, the *FSA* have banned over 100 mortgage brokers.~~ Breaches the *FCA* has identified as part of enforcements actions against mortgage brokers, have included:

…

The ~~*FSA* have~~ *FCA* has referred numerous cases to law enforcement, a number of which have resulted in criminal convictions.

…

5 Data security

…

5.2 Themes

…

Controls

5.2.3 …

Effective cyber practices

5.2.3A Self-assessment questions:

- Are critical systems and data backed up, and do you test backup recovery processes regularly?
- Are you able to restore services in the event of an incident?
- Are network and computer security systems, software and applications kept up-to-date and regularly patched? Do you make sure your computer network and information systems are configured to prevent unauthorised access?
- How do you manage user and device credentials? Do you ensure that staff use strong passwords when logging on to hardware and software? Are the default administrator credentials for all devices changed?
- Is two-factor authentication used where the confidentiality of the data is most crucial?
- How do you protect sensitive data that is stored or in transit? Do you use encryption software to protect your critical information from unauthorised access?

Examples of good practice	Examples of poor practice
	• Using weak or easy to guess passwords or creating passwords from familiar details.
• The firm carries out regular vulnerability assessments and patching.	• Poor physical management and/or control of devices.
• The firm carries out regular security testing.	• Not setting out appropriate user privileges on access to resources on the firm's network, data storages or applications.
• An application programming interface (API) allows different software to communicate with each other and has security measures in place.	• Not encrypting data at storage or between networks.
	• Not updating devices, software and operating systems with the latest security patches.
	• Not properly vetting third-party systems and vendors.

	• Not employing multi-factor authentication for devices, systems and services.
	• Insufficient staff training around social engineering and vishing and phishing campaigns.

…

Case study – protecting customers' accounts from criminals

5.2.4 …

For more, see the ~~*FSA's*~~ *FCA's* press release:
~~www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml~~

https://www.fca.org.uk/news/press-releases/fsa-fines-norwich-union-life-%C2%A3126m-exposing-its-customers-risk-fraud

Case study – data security failings

5.2.5 …

The ~~*FSA's*~~ *FCA's* press release has more details:

~~**http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/134.shtml**~~

https://www.fca.org.uk/news/press-releases/fsa-fines-zurich-insurance-%C2%A32275000-following-loss-46000-policy-holders-personal.

…

5.4.1 To find out more, see:

- the website of the Information Commissioner's Office: www.ico.org.uk.
- National Syber Security Centre, 10 Steps to Cyber Security: https://www.ncsc.gov.uk/collection/10-steps/data-security

…

6 Bribery and corruption

…

6.2 Themes

…

Case study – corruption risk

6.2.5 ~~In January 2009, Aon Limited, an insurance intermediary based in the UK, was fined £5.25m for failures in its anti-bribery systems and controls.~~

~~The firm made suspicious payments totalling $7m to overseas firms and individuals who helped generate business in higher risk jurisdictions. Weak controls surrounding these payments to third parties meant the firm failed to question their nature and purpose when it ought to have been reasonably obvious to it that there was a significant corruption risk.~~

- ~~Aon Limited failed properly to assess the risks involved in its dealings with overseas third parties and implement effective controls to mitigate those risks.~~
- ~~Its payment procedures did not require adequate levels of due diligence to be carried out.~~
- ~~Its authorisation process did not take into account the higher levels of risk to which certain parts of its business were exposed in the countries in which they operated.~~
- ~~After establishment, neither relationships nor payments were routinely reviewed or monitored.~~
- ~~Aon Limited did not provide relevant staff with sufficient guidance or training on the bribery and corruption risks involved in dealings with overseas third parties.~~
- ~~It failed to ensure that the committees it appointed to oversee these risks received relevant management information or routinely assessed whether bribery and corruption risks were being managed effectively.~~

~~See the *FSA's* press release: www.fsa.gov.uk/pages/Library/Communication/PR/2009/004.shtml~~

In 2020, the *FCA* and the *PRA* fined a global investment bank a total of £96.6m (US$126m) for risk management failures connected to a Malaysian development company ('the company') and its role in 3 fundraising transactions for the company.

The bank failed to assess and manage risk to the standard that was required given the high-risk profile of the transactions and failed to assess risk factors on a sufficiently holistic basis. The bank also failed to address allegations of bribery in 2013 and failed to manage allegations of misconduct in connection with the company in 2015.

The bank breached a number of *FCA* and *PRA* principles and *rules*. In particular, the bank failed to:

- assess with due skill, care and diligence the risk factors that arose in each of the bond transactions on a sufficiently holistic basis;
- assess and manage the risk of the involvement in the bond transactions of a third party about which the bank had serious concerns;
- exercise due skill, care and diligence when managing allegations of bribery and misconduct in connection with the company and the third bond transaction; and
- record in sufficient detail the assessment and management of risk associated with the company bond transactions.

Case study – inadequate anti-bribery and corruption systems and controls

6.2.6 …

See the ~~*FSA's*~~ *FCA's* press release:
~~www.fsa.gov.uk/pages/Library/Communication/PR/2011/066.shtml.~~
https://www.fca.org.uk/news/press-releases/fsa-fines-willis-limited-%C2%A36895-million-anti-bribery-and-corruption-systems-and

Case study – third parties

6.2.7 In 2022, the *FCA* fined an insurance broker £7,881,700 for financial crime control failings, which in one instance allowed bribery of over $3m to take place. The firm failed to consider whether additional safeguards or approvals should be incorporated into processes in respect to overseas introducers engaged by another group entity, where the introduced business was placed by the firm in the London market. Among other issues, the firm's third-party risk assessments failed by not:

- ensuring that information held by employees who were either involved in negotiating the relationship with the third party or placing the business in the London market, including potential red flags, was brought to the attention of the company's 'know your customer' subcommittee or its financial crime team;
- ensuring that the other entity disclosed all material information about the third party to the financial crime team for review, consideration and action as necessary; and
- considering whether additional monitoring and oversight of third parties, in accordance with firm's process, was appropriate.

…

7 Sanctions, ~~and~~ asset freezes and proliferation financing

7.1 Introduction

7.1.1 **Who should read this chapter?** All firms are required to comply with the UK's financial sanctions regime. The *FCA's* role is to ensure that the firms it supervises have adequate systems and controls to do so. As such, this chapter applies to **all firms** subject to the financial crime rules in *SYSC* 3.2.6R or *SYSC* 6.1.1R. It also applies to **e-money institutions and payment institutions and the cryptoasset sector** within our supervisory scope.

7.1.2 Firms' systems and controls should also address, where relevant, the risks they face from weapons proliferators, although these risks will be very low for the majority of ~~*FSA*-supervised~~ *FCA*-supervised firms. *FCG* 7.2.5G, which looks at weapons proliferation, applies to **banks carrying out trade finance business** ~~and those engaged in other activities, such as **project finance** and **insurance**, for whom the risks are greatest~~ all firms subject to our supervision.

…

7.1.5 All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the ~~EU an~~d UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

Under Principle 11 (*PRIN* 2.1.1R), we expect authorised firms to notify us if they (or their group companies, *approved persons*, *senior management functions*, *appointed representatives* (ARs) and *agents*) are subject to sanctions.

For firms such as *electronic money institutions*, payment services firms, *cryptoasset businesses* and Annex I financial institutions, this is regarded as a material change of circumstance and we expect to be informed if you or any connected entities are subject to sanctions.

7.1.5A The Office of Financial Sanctions (OFSI) within the Treasury helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom. OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations~~, the European Union~~ and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify OFSI in accordance with the relevant provisions. OFSI have published guidance on complying with UK obligations and this is available on their website. See https://www.gov.uk/government/publications/financial-sanctions-faqs.

Firms should also consider whether they should report sanctions breaches to the *FCA*. *SUP* 15.3 contains general notification requirements. Firms are required to tell us, for example, about significant rule breaches (see *SUP* 15.3.11R(1)). Firms should therefore consider whether a sanctions breach is the result of any matter within the scope of *SUP* 15.3 – for example, a significant failure in their financial crime systems and controls.

…

7.2 Themes

The guidance set out in *FCG* 2.2 (Themes) and *FCG* 2.3 (Further guidance) also applies to sanctions.

Governance

7.2.1 The guidance in *FCG* 2.2.1G on governance in relation to financial crime also applies to sanctions.

~~Senior management should be sufficiently aware of the firm's obligations regarding financial sanctions to enable them to discharge their functions effectively.~~

We expect senior management to take clear responsibility for managing sanctions risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are actively engaged in the firm's approach to addressing the risks of non-compliance with UK financial sanctions. Where they identify gaps, they should remediate them.

Self-assessment questions:

- …
- ~~How does the firm **monitor performance**? (For example, statistical or narrative reports on matches or breaches.)~~
- How are **senior management** kept **up to date** with sanctions compliance issues?
- Does the firm's organisational structure with respect to sanctions compliance across **different jurisdictions** promote a **coordinated approach and accountability**?
- Does the firm have **evidence** that sanctions issues are **escalated** where warranted?
- Where sanctions controls processes rely on resource external to the firm, is there **appropriate oversight** and **understanding** of that resource?

Examples of good practice	Examples of poor practice
• An individual of **sufficient authority** is responsible for overseeing the firm's adherence to the sanctions regime.	• The firm believes payments to sanctioned individuals and entities are **permitted** when the sums are small. Without a licence from ~~the Asset Freezing Unit~~ OFSI, this could be a **criminal offence**.
	• Multinational firms **lack** the **communication** between global and regional sanctions teams necessary to ensure compliance with UK sanctions laws, regulations and guidance.
…	

…

Management information (MI)

7.2.1A The guidance in *FCG* 2.2.2G on MI in relation to financial crime also applies to sanctions.

Senior management should be sufficiently aware of the firm's obligations regarding financial sanctions to enable them to discharge their functions effectively.

Self-assessment questions:

- How does your firm **monitor performance**? (For example, statistical or narrative reports on matches or breaches.)
- Does **regular and ad hoc MI** provide senior management with a clear understanding of the firm's sanctions compliance risk?
- Is the MI produced **calibrated** to UK sanctions regimes?

Risk assessment

7.2.2 The guidance in *FCG* 2.2.4G on risk assessment in relation to financial crime also applies to sanctions.

A firm should consider which areas of its business;

- are most likely to provide services or resources to individuals or entities on the Consolidated List;
- are owned and controlled by individuals or entities on the Consolidated List;
- engage in services or transactions prohibited under the UK financial sanctions regime; or
- rely on prohibited suppliers, intermediaries or counterparties.

Self-assessment questions:

- Does your firm have a clear view on where within the firm breaches are most likely to occur? (This may cover different business lines, sales channels, customer types, geographical locations, etc.)
- How is the risk assessment **kept up to date**, particularly after the firm enters a new jurisdiction ~~or,~~ introduces a new product or where there are new developments in the sanctions landscape?
- Has senior management set a clear **risk appetite** in relation to its sanctions risks, including in its exposure to sanctioned persons, activities and countries?
- Does your firm have established **risk metrics** to help detect and manage its sanctions compliance exposure on an ongoing basis?
- Are there established **procedures** to identify and escalate new sanctions risk events, such as new sanctions regimes, sanctioned activities and evasion typologies?

- Is your firm utilising available guidance and resources on **new and emerging** sanctions evasion typologies?

Examples of good practice	Examples of poor practice
…	
• A small firm is **aware** of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.	• The firm assumes financial sanctions **only apply to money transfers** and so has not assessed its risks.
• The firm conducts **contingency planning**, taking a proactive approach to identifying sanctions exposure and is conducting exposure assessments and scenario planning. The firm updates business-wide and customer risk assessments to **account for changes** in the nature and type of sanctions measures.	
• The firm **performs lessons learned** exercises following sanctions developments to improve its readiness to respond to future events.	
• The firm engages with **public-private partnerships and private-private partnerships** to gather insights on the latest typologies and additional controls that might be relevant and share its own best practice examples.	

Customer due diligence checks

7.2.2A Effective customer due diligence (CDD) and know your customer (KYC) assessments are a cornerstone of effective compliance with sanctions requirements.

Examples of good practice	Examples of poor practice

• Sanctions risk is **proactively** included into the firm's CDD process.	• The firm has **low quality** CDD and KYC assessments and **review backlogs**, raising the risk of not identifying sanctioned individuals and entities.
• The firm's CDD identifies and screens **all relevant parties**.	• The firm's CDD processes are **unable to identify** connected parties and corporate structures that may be subject to sanctions.
• The firm's customer onboarding and due diligence processes **identify** customers who make use of **corporate vehicles** to obscure ownership or source of funds.	• The firm's CDD **does not articulate** full ownership structures of entities and the firm is unable to show that it is screening all relevant parties.
• The firm is able to **identify** activity that is **not in line with the customer profile** or is otherwise **suspicious** and ensures that these are reported quickly to the nominated officer for timely consideration.	

Further guidance on good and bad practice relating to CDD checks are covered in *FCG* 3.2.4.

Screening customers ~~against sanctions lists~~, counterparties and payments

7.2.3 A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. Although screening itself is not a legal requirement, screening new customers, counterparties and payments against the Consolidated List, and screening existing customers when new names are added to the list, helps to ensure that firms will not breach the sanctions regime. (Some firms may knowingly continue to retain customers who are listed under UK sanctions: this is permitted if OFSI has granted a licence.)

Self-assessment questions:

- …
- How does the firm become **aware of changes** to the Consolidated List? (Are there manual or automated systems? Are customer lists rescreened after each update is issued?)
- Does your firm have a **clear policy** on which customers, counterparties and payments are subject to screening, and what related data is subject to screening?

- Does your firm have **service level agreements** that cover how quickly it updates its sanctions screening lists following updates to the Consolidated List that are appropriate to the sanctions risks of its business?
- Does your firm **evaluate** its **screening capabilities** so that its screening system is adequately calibrated for its needs and calibrated to monitor the UK sanctions regime? Do you regularly **test/measure** the effectiveness of the system?
- Is the team responsible for sanctions compliance properly **resourced and skilled** to effectively perform sanctions screening?
- If using an outsourced service, does your firm have appropriate **control and oversight** of its sanctions screening controls?

Examples of good practice	Examples of poor practice
…	
• There are quality control checks over **manual screening**.	• Where a firm uses automated systems, it does not understand how to **calibrate** them and does not check whether the number of hits is unexpectedly high or low.
• The firm **understands** the screening tool and how it is calibrated, and is able to demonstrate that it is appropriate to the firm's risk exposure.	• Calibration is **not adequately tailored** and the system is either too sensitive or not sensitive enough. This may result in name variations not being detected, for example.
• The firm is able to show the controls in place to **measure the effectiveness** of the system, thresholds and parameters – for instance, with sample testing and tuning.	• There is **limited or no understanding** by the firm about how a third-party tool is calibrated and when lists are updated.
• Where a firm uses automated systems, these can make '**fuzzy matches**' (e.g. able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.). The firm continually seeks ways to enhance the system to help identify sanctions evasion.	• An insurance company **only screens when claims** are made on a policy.
…	

• Where the firm maintains an account for a listed individual or entity, the status of this account is **clearly flagged** to staff.	• Updating from the Consolidated List is **haphazard**. Some business units use out-of-date lists.
• A firm only ~~places faith in~~ relies on **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy ~~themselves~~ itself this is appropriate.	• The firm is **overly reliant** on a third-party provider screening solution, with no oversight. The firm has **no means** of monitoring payment instructions.
• The screening tool is **calibrated and tailored** to the firm's **risk** and appropriateness for the **UK sanctions regime**. Customers and their transactions are screened against relevant updated sanctions lists and effective re-screening is in place to identify activity that may indicate sanctions breaches.	
• Where **blockchain analytics** solutions are deployed, the firm ensures that compliance teams **understand** how these capabilities can be best used to identify transactions linked to higher risk wallet addresses.	
• The firm's sanctions teams are adequately **resourced** to avoid backlogs in sanctions screening and are able to react to those at pace.	• The firm **lacks proper resources** and **expertise** to ensure effective screening, it has significant backlogs and faces the risk of non-compliance with its obligations.
	• Increased volumes and pressure on sanctions teams **prevent** firms from taking **appropriate and timely action** for true positive alerts and increase the risk of errors. There is a lack of clarity around prioritisation of alerts, internal service level agreements and governance.

Evasion detection and investigation

7.2.3A A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. However, simple screening of names against

the Consolidated List may not always identify potential sanctions evasion involving third parties and alternative detection techniques may be needed.

Self-assessment questions:

- Does your firm understand potential sanctions **evasion typologies** relevant to its business and has it considered how to detect them?
- Has your firm considered whether **additional procedures are needed** to identify potential sanctions evasion?

Examples of good practice	Examples of poor practice
• The firm is using techniques such as data analytics to identify customers who may be close associates or dependents or have transactional links with designated persons, and so may **represent a higher risk** of sanctions non-compliance.	

Asset freezing and licenses

7.2.3B When a financial sanction is an asset freeze, generally the funds and economic resources belonging to or owned, held or controlled by a designated person are to be frozen immediately by the person in possession or control of them, unless there is an exception in the legislation they can rely on, or they have a licence from OFSI.

Self-assessment questions:

- Does your firm have **clear policies and procedures** as to when funds and economic resources are frozen or released?
- Have you assessed how any frozen funds and economic resources in your firm's possession or control are **maintained in compliance** with the UK sanctions regime?
- Does your firm have clear policies and procedures to **assess, utilise and monitor** the use of OFSI licences and statutory exceptions?

Reporting and assessing potential sanctions breaches

7.2.3C Relevant firms are required to report to OFSI where they know or have reasonable cause to suspect a breach of financial sanctions, and notify OFSI if:

- a person they are dealing with, directly or indirectly, is a designated person;
- they hold any frozen assets; or
- they discover or suspect any breach while conducting their business.

In line with *Principle* 11, *SUP* 15.3.8G(2) and *FCG* 7, firms must consider whether they need to notify us – for example, whether potential breaches of sanctions resulted from a significant failure in their systems and controls.

Self-assessment questions:

- Is there a clear procedure that sets out what to do if a potential **sanctions breach** is identified? (This might cover, for example, alerting senior management, OFSI and the *FCA*, and giving consideration to whether to submit a Suspicious Activity Report).
- Does your firm consider the **root causes** of any potential sanctions breaches and consider the implications for its policies and procedures?

Examples of good practice	Examples of poor practice
• The firm undertakes **a root cause analysis** of potential sanctions breaches and uses them to update its sanctions controls.	The firm **does not report a breach** of the financial sanctions regime to OFSI. This could be a criminal offence.
• After a breach, as well as meeting its formal obligation **to notify OFSI**, the firm **reports the breach to the *FCA***. *SUP* 15.3 contains general notification requirements. Firms are required to tell us about significant *rule* breaches (see *SUP* 15.3.11R(1)), such as a significant failure in their financial crime systems and controls.	
• Breaches and related systems and controls deficiencies **are reported** to the *FCA* once identified, within reasonable timelines.	

…

Weapons proliferation

7.2.5 Alongside financial sanctions, the government imposes controls on certain types of trade in order to achieve foreign policy objectives. The export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Firms' systems and controls, and policies and procedures should address and mitigate the proliferation risks they face. Firms are also required to carry out proliferation financing risk assessments under Regulation 18A of the Money Laundering Regulations 2022, either as part of the existing practice-wide risk assessment or as a standalone document.

…

…

~~Case study – deficient sanctions systems and controls~~

7.2.6 ~~In August 2010, the *FSA* fined Royal Bank of Scotland (RBS) £5.6m for deficiencies in its systems and controls to prevent breaches of UK financial sanctions.~~

- ~~RBS failed adequately to screen its customers – and the payments they made and received – against the sanctions list, thereby running the risk that it could have facilitated payments to or from sanctioned people and organisations.~~
- ~~The bank did not, for example, screen cross-border payments made by its customers in sterling or euros.~~
- ~~It also failed to ensure its 'fuzzy matching' software remained effective, and, in many cases, did not screen the names of directors and beneficial owners of customer companies.~~

~~The failings led the *FSA* to conclude that RBS had breached the Money Laundering Regulations 2007, and our penalty was imposed under that legislation – a first for the *FSA*.~~

~~For more information see the *FSA's* press release: www.fsa.gov.uk/pages/Library/Communication/PR/2010/130.shtm.~~ [deleted]

7.3 Further guidance

7.3.1 *FCTR* contains the following additional material on sanctions and assets freezes:

- *FCTR* 8 summarises the findings of the ~~*FSA's*~~ *FCA's* thematic review ~~Financial~~ of financial services firms' approach to UK financial sanctions and includes guidance on

  …

- …

7.4 Sources of further information

7.4.1 To find out more on financial sanctions, see:

- …
- Part III of the Joint Money Laundering Steering Group's guidance, which is a chief source of guidance for firms on this topic: www.jmlsg.org.uk
- OFSI UK Financial Sanctions Guidance: https://www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance
- Alerts published by the National Economic Crime Centre (NECC). https://www.nationalcrimeagency.gov.uk/who-we-are/publications/

- FCA Sanctions webpages – these pages include our latest updates and details on how to report sanctions breaches to us: https://www.fca.org.uk/russian-invasion-ukraine and https://www.fca.org.uk/firms/financial-crime/financial-sanctions.

7.4.2 To find out more on trade sanctions and proliferation, see:

- …
- The NCA's website, which contains guidelines on how to report suspicions related to weapons proliferation: ~~http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/57-sar-guidance-notes~~ https://www.nationalcrimeagency.gov.uk/who-we-are/publications/171-sar-guidance-notes/file
- The FATF ~~website. In June 2008, FATF launched a 'Proliferation Financing Report' that includes case studies of past proliferation cases, including some involving UK banks. This was followed up with a report in February 2010~~ guidance on proliferation financing:
  - ~~https://www.fatfgafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf~~. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf
  - ~~http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.~~ https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf.

…

Annex Common terms

Annex 1 Common terms

Annex 1 …

Term	Meaning
…	
~~EEA firms~~	~~Firms from the European Economic Area (EEA) which passport into the UK are authorised persons. This means, generally speaking, EEA firms who carry on relevant business from a UK branch will be subject to the requirements of the *Handbook* and of the *Money Laundering Regulations*. However, an EEA firm that only provides services on a cross-border basis (and so~~

	~~does not have a UK branch) will not be subject to the *Money Laundering Regulations*, unless it carries on its business through representatives who are temporarily located in the UK.~~
…	
equivalent jurisdiction	A jurisdiction ~~(other than an EEA state)~~ whose law contains equivalent provisions to those ~~contained in the Fourth Money Laundering Directive~~ in the UK. The JMLSG has prepared guidance for firms on how to identify which jurisdictions are equivalent. Equivalent jurisdictions are significant because it is a factor that a firm may consider when deciding whether to apply 'simplified due diligence' to financial institutions from these places. Firms can also rely on the customer due diligence checks undertaken by certain introducers from these jurisdictions (see 'reliance').
…	

Pub ref: 1-008254

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk