

Consultation Paper

CP26/38***

Financial Crime Guide Updates

October 2026

Contents

Chapter 1	Summary	Page 3
Chapter 2	Proposed changes	Page 6
Chapter 3	How to respond	Page 14
Annex 1	Questions in this paper	Page 15
Annex 2	Cost benefit analysis	Page 16
Annex 3	Compatibility statement	Page 17
Annex 4	Abbreviations used in this paper	Page 22
Appendix 1	Draft Handbook text	

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 0207 066 1000



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

See all our latest press releases, consultations and speeches.

Chapter 1

Summary

- 1.1** Financial crime is becoming more sophisticated and complex. We're consulting on changes to our Financial Crime Guide (the Guide) to help firms assess and strengthen their financial crime systems and controls.
- 1.2** Financial crime causes wide-ranging harm: it damages lives and livelihoods, enables serious and organised crime, undermines trust in the financial system and weakens the wider economy. Tackling it is one of our priorities and requires a coordinated effort across industry, government, law enforcement and regulators. Firms are essential partners in that collective effort. Their work to detect, prevent and disrupt financial crime helps protect consumers and safeguard the integrity of the financial system.
- 1.3** The updates we propose are informed by insights from our supervision and wider developments. We want the Guide to continue to help firms understand our expectations, strengthen their financial crime systems and controls and support their efforts to detect, prevent and disrupt financial crime.
- 1.4** The Guide includes self-assessment questions and examples of good and poor practice drawn from our supervisory work and wider financial crime publications.
- 1.5** The Guide does not contain rules nor impose any new requirements. We expect firms to have read and considered it, using it as well as their own judgement to establish effective policies and controls.
- 1.6** Firms should factor in the UK's System Priorities to demonstrate how they counter financial crime risk. The System Priorities framework is developing with focus on delivering more through Public Private Partnership.
- 1.7** For further information on how these changes aim to prevent harm and how the consultation aligns with FCA objectives, see paragraph 1.13 and Chapter 2.
- 1.8** This CP should be read by:
- all FCA financial crime supervised firms, including firms we supervise under The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), such as Annex I Financial Institutions and cryptoasset businesses.
- 1.9** The CP may also be of interest to:
- individuals and organisations working with firms subject to our financial crime and MLRs supervision
 - financial services trade organisations and professional bodies
 - any other parties interested in our financial crime supervision, such as non-governmental organisations working on financial crime prevention, or academics

What we want to update

1.10 We want the Guide to be clear, reflect our recent findings, and help firms identify and assess the right financial crime controls.

1.11 We propose changes to the following areas:

Fraud: Updates to reflect supervisory expectations and lessons from our multi-firm work on authorised push payment (APP) fraud and money mules, responding to industry feedback for more guidance.

Cryptoassets: From 25 October 2027, firms carrying out certain cryptoasset activities in the UK will need to be authorised by us under the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026. The Guide will help firms meet our expectations when developing and maintaining financial crime systems and controls.

Financial and trade sanctions: The UK's sanctions regime has evolved since the Guide was last updated, and since the Office of Trade Sanctions Implementation (OTSI) was established. We propose to update this section to reflect these developments and include examples of good and poor practice drawn from our supervisory work.

Proliferation financing: Supervisory work has highlighted the need for enhanced guidance on proliferation financing risks and controls, including further detail on our expectations for firms.

Data security: We want the guidance to keep pace with today's financial crime and cyber risks, data protection legislation, governance and crisis communication, and emerging risks associated with AI, synthetic identity fraud and digital assets.

Financial crime system and controls: Clarifying our expectations for firms using Banking as a Service (BaaS) delivery models, including where services are outsourced, white labelled or provided through embedded finance partnerships.

Money laundering and terrorist financing: Updates so that the Guide remains current and reflects developments in industry practice, such as electronic verification, third party tools and outsourcing arrangements, and clarifying the importance of co-operation and information sharing.

Consequential changes: Updates to the Guide, including reflecting recent changes to the MLRs that came into force in June 2026, updating expired links and references (including references to European Union legislation), and refreshing case studies.

1.12 Further details are in Chapters 2-3 and Appendix 1.

Intended outcomes

- 1.13** The proposed changes are to help firms:
- **reduce financial crime:** We want to make sure that firms and markets are not used for financial crime. These changes give firms guidance on how they might evaluate or set up their systems and controls.
 - **maintain confidence in the financial system:** Confidence in the UK financial system depends on firms preventing harm to the public. We have proposed changes so that the Guide continues to reflect our expectations, and protects confidence in and the integrity of the financial system.
 - **protect consumers:** Effective financial crime systems and controls protect consumers from harm. The proposed changes reinforce our expectations that firms maintain controls that are proportionate to the risks they face.

Outcomes and measuring success

- 1.14** We will evaluate the impact of the consultation by analysing engagement and feedback on the proposed changes.
- 1.15** We will continue to update the guidance in line with our supervisory findings and publications. We also welcome feedback on chapters from stakeholders on chapters or areas not addressed in this CP that they consider we should focus on in future.

Next steps

- 1.16** We welcome your feedback on our proposed guidance in Appendix 1 by 24 December 2026. The specific questions for feedback are in Annex 1.
- 1.17** You can submit your responses via the form on our website. If you are not able to use the form, write to us at CP26-38@fca.org.uk.
- 1.18** We will consider your comments and 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 updates to the Guide.

Chapter 2

Proposed changes

Fraud

- 2.1** Fraud has significant financial and emotional consequences for victims. It also undermines security and trust in the UK financial system. In recent years, government, law enforcement, regulators and industry have stepped up efforts to tackle it.
- 2.2** We have assessed systems and controls for detecting and preventing authorised push payment (APP) fraud and money mule activity at Payment Service Providers (PSPs), including retail banks, and payments and e-money firms. We have heard repeated calls from industry for more guidance on fraud.
- 2.3** So we propose making updates to Chapter 4 – Fraud. These will incorporate the findings of systems and controls publications, including:
- Anti-fraud controls and complaint handling in firms (with a focus on APP fraud)
 - Proceeds of fraud – detecting and preventing money mules
 - Firms' use of the National Fraud Database (NFD) and money mule account detection tools
 - Combating romance fraud – prevention, detection and supporting victims

Our updated guidance focuses on APP fraud and money mule systems and controls, to help the firms we regulate meet their financial crime obligations.

The new section on APP fraud and money mules is structured around three areas: onboarding, monitoring and reporting. The updated guidance is focussed on APP fraud as the overarching typology and does not reference specific fraud types associated with APP fraud. To reflect this, we have incorporated the guidance on investment fraud into the updated APP fraud section and set out that firms should be considering the risks associated with different APP fraud typologies as part of its anti-fraud systems and controls. We remain committed to tackling investment fraud:

- we have introduced the Firm Checker tool for consumers to check firms are authorised by us and have the permissions to provide the services they want before making investments
- we publish the FCA warning list of unauthorised firms
- we publish information to help consumers protect themselves from scams
- we have led international action to stop illegal influencers putting consumers' money at risk.

Onboarding

- We expect firms to consider the onboarding checks that will help mitigate both the risks of fraud and of moving the proceeds of fraud.
- We have shared examples of good and poor practice for onboarding. They include:
 - Good practice: where firms have built a holistic view of the customer, reviewed a range of sources to aid behavioural profiling, used fraud databases, identified customer vulnerability, and implemented checks to identify synthetic or counterfeit documentation.
 - Poor practice: failing to keep accurate records of onboarding checks, completing basic checks that do not inform a holistic picture of the customer, and only being aware of customer vulnerabilities after a fraud has occurred.

Monitoring

- Swift and proactive detection of unusual activity helps firms spot weaknesses in systems and controls that fraudsters might exploit.
- We have included some potential APP fraud indicators, such as changes in behavioural biometrics, changes in expected account turnover, negative Confirmation of Payee (COP) results, creation of new payees with high value transactions, and customers using increasingly desperate tones in communications.
- We have included some money mule activity indicators, such as including unexpected or unexplained deposits, rapid dispersal of funds, changes in dormant accounts, online banking credentials changing, and changes to device or contact details are inconsistent with the firm's knowledge of the customer.
- There are examples of good and poor practice for APP fraud and money mule monitoring. They include:
 - Good practice: monitoring inbound and outbound transactions, reviewing and testing transaction monitoring alerts, customer warnings, prompt investigation of money mule alerts, and policies and procedures for the firm's response to money mules.
 - Poor practice: inadequate staff training to identify APP fraud or money mule indicators, lack of feedback loops on updates to systems and controls, a focus on outbound transaction monitoring only, failing to promptly implement new transaction monitoring alerts, and failing to review or assess the impact of customer warnings.

Reporting

- We expect firms to have policies and procedures for reporting instances of fraud to the authorities. Reporting on fraud data, as well as wider information sharing, at an industry level plays a key role in tackling fraud across the whole system. We encourage firms to contribute to data sharing initiatives, in support of the wider cross-system approach for tackling fraud.
- There are examples of good and poor practice for APP fraud and money mule reporting. They include:

- Good practice: identifying APP fraud trends and sharing them through cross-system initiatives for data sharing, sharing key information promptly and efficiently, assessing money mule cases individually, and promptly reporting relevant cases to industry databases.
- Poor practice: failing to act after receiving specific intelligence, and failing to keep comprehensive records in relation to decisions to file (or not to file) to fraud databases.

- 2.4** In addition, we propose to build on existing fraud guidance by strengthening content relating to fraud risk assessments, governance and oversight, and using management information and assurance to identify, monitor and escalate risks.
- 2.5** We propose to include examples of how firms may respond to evolving fraud typologies, through staff training, analytical tools and fraud prevention controls.
- 2.6** These updates complement and are consistent with the UK's wider fraud policy and strategy. This covers: APP scams reimbursement requirements, the Payment Services (Amendment) Regulations 2024 (slowing down outbound payment processing where there are reasonable grounds to suspect fraud), system prioritisation to tackle the biggest economic threats under Economic Crime Plan 2 (ECP2), and the UK Fraud Strategy 2026-2029.

Question 1: **At the time of publication, investment fraud was increasing: UK Finance data showed a 26% rise in cases and a 40% increase in losses between 2024 and 2025. Are there particular challenges in detecting and preventing investment fraud through systems and controls? What guidance on systems and controls for investment fraud should be included alongside the broader APP fraud guidance?**

Cryptoassets

- 2.7** Since January 2020, cryptoasset businesses operating in the UK, defined in the MLRs as cryptoasset exchange providers or custodian wallet providers, have been required to register with the FCA. Following the Financial Services and Markets Act (Cryptoasset) Regulations 2026 (Cryptoasset Regulations), from 25 October 2027, firms carrying out certain regulated cryptoasset activities by way of business in the UK will need to be authorised by us and comply with our financial crime rules (as published in PS26/13).
- 2.8** Firms in scope of the Cryptoasset Regulations will still need to comply with their obligations under the MLRs, as well as other financial crime legislation such as the Terrorism Act 2000 and Proceeds of Crime Act 2002.
- 2.9** Many firms will be new to these regulations, and we want our guidance to help them understand and be aware of compliance with financial crime expectations under

Financial Services and Markets Act 2000 and the MLRs. Our proposed updates will give examples of good and poor practice, helping firms implement systems and controls to prepare for applications.

- 2.10** The 2025 National Risk Assessment ranked the risk for money laundering as 'high' and for terrorist financing as 'medium' for cryptoassets. The cross-border and fast-moving nature of blockchain and cryptoasset transactions make detection and enforcement uniquely difficult. Our proposed updates to the Guide clarify our expectations that firms adopt a risk-based approach to identifying and mitigating these risks.
- 2.11** Our proposed guidance includes:
- Good and poor practice examples on the triggers for enhanced due diligence, reflecting the financial crime risks faced by firms engaging with cryptoassets.
 - Good and poor practice examples of how firms meet our expectations on systems and controls, such as for onboarding and monitoring, and the use of blockchain analytics for firms engaging in cryptoasset activities.
 - Further guidance on firms' obligations for complying with the Travel Rule.
- 2.12** We are reminding firms of our expectations on governance. We expect all firms, including start-ups, to proactively monitor and adapt their approach as their business grows and matures.
- 2.13** In addition, we are proposing to add a self-assessment question to help firms consider whether their policies, procedures and staff training adequately distinguish between obligations under the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

Financial sanctions and trade sanctions

- 2.14** All firms should understand how their business may be exposed to sanctions risk and ensure their controls are proportionate to that exposure. Our supervisory work has shown that they'd benefit from more guidance on assessing their exposure and testing their controls.
- 2.15** We are proposing updates to Chapter 7 of the Guide to set out our expectations and examples of good and poor practice. In particular, we propose to cover trade alongside financial sanctions, reflecting developments in the UK's sanctions framework including the establishment of OTSI.
- 2.16** The updates are to help firms consider their exposure to risk from their customers, counterparties, intermediaries, jurisdictions, goods, services, transactions, payments and payment messages. The guidance will help them assess their risk assessments, customer due diligence (CDD), screening, monitoring and reporting.

- 2.17** We propose to update references to relevant authorities. The revised chapter will refer to OFSI for financial sanctions, OTSI for trade sanctions, HMRC where suspected breaches relate to export controls or customs matters, and to us where issues may indicate weaknesses in a firm's financial crime systems and controls.
- 2.18** The revised chapter will improve guidance on governance, management information, risk assessment, CDD, screening, evasion detection, asset freezing, licensing and breach reporting. It will reorganise some existing material so that the chapter is easier to follow and refreshed with more recent FCA enforcement examples.
- 2.19** The specific guidance includes:
- Explaining how firms may be exposed to financial and trade sanctions risk through their business relationships, activities and transaction flows.
 - Clarifying the respective roles of OFSI, OTSI, HMRC and the FCA, including the circumstances in which matters may need to be reported to each authority.
 - Strengthening guidance on governance and management information, including senior management oversight, escalation, training and the monitoring of sanctions controls.
 - Expanding risk assessment guidance to address matters such as sanctions circumvention, intermediary countries and sectoral and trade sanctions.
 - Enhancing guidance on CDD and KYC, including the consideration of ownership structures, connected parties, counterparties and relevant trade information.
 - Reorganising the screening material to distinguish more clearly between screening policies, sanctions-list management, system calibration, testing and alert management.
 - Clarifying firms' responsibilities when using third-party screening tools or outsourced arrangements, including oversight of vendor-configured settings and the timely, complete and accurate implementation of sanctions-list data.
 - Encouraging firms to consider monitoring beyond name screening, including risks associated with goods, vessels, ports, services and jurisdictions.
 - Developing guidance on detecting sanctions evasion through appropriate typologies, data analysis, thematic review and transaction monitoring.
 - Setting out practices for managing screening alerts, including resourcing, backlogs, internal decision-making standards and audit trails.
 - Updating guidance on asset freezing, licensing and suspected breaches, including escalation, root cause analysis and reporting to the relevant authorities.

Proliferation financing

- 2.20** We propose to update the proliferation financing material in Chapter 7. The revisions recognise that proliferation financing may involve mechanisms similar to sanctions evasion and clarifies how firms might manage the risk through existing controls.
- 2.21** We propose to add self-assessment questions and examples of good and poor practice covering strategic export controls, dual-use and military goods, reporting and escalation procedures, the integration of proliferation financing into risk assessments, and how firms respond to published typologies when assessing their exposure to proliferation financing risks.
- 2.22** It includes:
- explaining how sanctions controls may help manage proliferation financing risk
 - guidance on higher-risk goods and activities, including strategic export controls, dual-use goods and military goods
 - guidance on documented reporting and escalation procedures for suspected proliferation financing breaches
 - updated good practice examples such as integrating proliferation financing risk into risk assessments, reviewing exposure after typology publications, and avoiding failures to incorporate PF risk into onboarding, CDD, screening and transaction monitoring. We also included examples of poor practice
- 2.23** In addition, if a new Proliferation Finance National Risk Assessment is published before we have finalised the Guide, we'll include a reference to it.

Data security

- 2.24** We propose to update the Data Security guidance, so it reflects today's financial crime and cyber risk landscape. Changes include:
- updating outdated legislative references to align with the Data Protection Act 2018 and UK GDPR
 - strengthening governance expectations by incorporating board involvement, improved crisis communication; and
 - refreshing self-assessment material covering AI, synthetic identity fraud and digital asset-related risk
- 2.25** This will help firms assess whether their systems and controls are effective. The case studies and the 'five fallacies of data loss and identify fraud' section will be refreshed to reflect modern threats, including deepfakes. We'll include learnings from recent enforcement cases, so that firms can benchmark themselves against risks.

Financial crime systems and controls

- 2.26** We propose to set out how financial crime obligations apply in Banking as a Service (BaaS) and embedded finance arrangements, both where the BaaS user is another regulated firm and where it is unregulated. The guidance reinforces that regulated firms are accountable for maintaining effective systems and controls across the delivery chain, including where activities are outsourced, white-labelled or delivered through embedded finance models.

Money laundering and terrorist financing

- 2.27** Firms are increasingly using AI and other third-party tools in their financial crime systems and controls. They must apply governance and oversight to these and remain accountable for managing the financial crime risks they present. The tools must be proportionate to the firm's risk profile and risk appetite, and subject to testing and validation.
- 2.28** We are proposing additions to the Guide so that it remains current and aligned with industry practice, such as expanded guidance on electronic verification. We have added examples of good and poor practice relating to notification obligations for PSPs and Intermediary Service Providers where there are repeated failures to comply with fund transfer requirements involving electronic transmission. We have also updated related terminology, including replacing references to Production Orders with Investigative Court Orders.
- 2.29** The banking and financial sector is critical national infrastructure, relied upon by businesses and the public every day. We have a duty to promote the resilience of the sector and its ability to withstand attempts to disrupt or deny services. We work closely with law enforcement agencies, regulators and other authorities to support stable, resilient and robust financial systems, maintained by effective co-operation and information sharing. We therefore propose to reinforce the importance of this between firms, regulators, law enforcement agencies and other relevant authorities.

Consequential changes

- 2.30** We are proposing other changes to keep the Guide up to date, as a consequence of wider changes. These are:
- Updating it to reflect amendments to the MLRs introduced in June 2026.
 - Removing references to European Union rules and supervisory authorities to keep it consistent with changes following the UK's exit from the EU.
 - Refreshing links and more recent examples of outcomes on financial crime.
 - Including more links to useful material for firms to consult when conducting or reviewing their systems and controls.
 - Making other minor drafting changes.

- Question 2:** Do you agree with the suggested drafting as set out in this Consultation Paper? If not, please explain why.
- Question 3:** For future iterations, which chapters in the Guide or financial crime topics not included would you like us to cover?
- Question 4:** Do you foresee any unintended consequences from the proposals?
- Question 5:** How could we improve our approach to developing and publishing financial crime guidance? We welcome feedback, ideas and suggestions on what firms would find useful and how we could engage with them, for example through online or in-person sessions?

Chapter 3

How to respond

We are asking for comments on this Consultation Paper (CP) by 24 December 2026 .

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

www.fca.org.uk/publications/consultation-papers/cp26-38-financial-crime-guide-updates

Or in writing to:

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

Telephone: 0207 066 0984

Email: cp26-38@fca.org.uk

To read how we will use your response and how it will be disclosed, visit: [Consultation responses: your confidentiality and personal data | FCA](#)

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

If you choose not to respond using our online form, please let us know whether you consent to your name and response being made available to the public.

Please be sure to let us know in what capacity you are responding. If you are responding 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).

Annex 1

Questions in this paper

- Question 1:** At the time of publication, investment fraud was increasing: UK Finance data showed a 26% rise in cases and a 40% increase in losses between 2024 and 2025. Are there particular challenges in detecting and preventing investment fraud through systems and controls? What guidance on systems and controls for investment fraud should be included alongside the broader APP fraud guidance?
- Question 2:** Do you agree with the suggested drafting as set out in this Consultation Paper? If not, please explain why.
- Question 3:** For future iterations, which chapters in the Guide or financial crime topics not included would you like us to cover?
- Question 4:** Do you foresee any unintended consequences from the proposals?
- Question 5:** How could we improve our approach to developing and publishing financial crime guidance? We welcome feedback, ideas and suggestions on what firms would find useful and how we could engage with them, for example through online or in-person sessions?

Annex 2

Cost benefit analysis

Introduction

- 1.** The Financial Services and Markets Act (2000) require 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.** However, FSMA does not require us to produce and publish a CBA when proposing guidance (see section 139A of FSMA on power of the FCA to give guidance and section 139B of FSMA on the meaning of general guidance). As set out in our Statement of Policy on CBAs we may produce a CBA for general guidance if a high-level assessment of the impact of the proposal identifies an element of novelty, which may be in effect prescriptive or prohibitive, that may result in significant costs being incurred.
- 3.** Our Statement of Policy on CBAs provides that a CBA is undertaken where changes to guidance are likely to result in significant costs. In this case, we do not consider that significant costs will arise. The proposed updates reflect existing regulatory expectations and established industry practice and are intended to clarify and update existing guidance, not introduce new requirements. We therefore do not expect the proposals to result in a material increase in the frequency of, or time spent on, compliance activities, nor do we expect them to result in material costs to consumers, materially alter the products and services provided by firms, or have a material impact on competition or the wider economy.
- 4.** The proposals in this consultation relate to general guidance as defined in section 139B of FSMA. As explained in FCG 1.1.7, the Guide contains general guidance that is not binding and a firm's departure from that guidance does not, of itself, indicate a breach of FCA rules. Therefore, we have not undertaken a CBA.

Annex 3

Compatibility statement

Compliance with legal requirements

1. This Annex records the FCA's compliance with a number of legal requirements applicable to the proposals in this consultation, including an explanation of the FCA's reasons for concluding that our proposals in this consultation are compatible with certain requirements under the Financial Services and Markets Act 2000 (FSMA).
2. Section 1B(1) of FSMA requires that the FCA, when discharging its general functions, as far as reasonably possible, act in a way which is compatible with its strategic objective and advances one or more of its operational objectives, and its general duty under section 1B(5)(a) of FSMA to have regard to the regulatory principles in section 3B of FSMA.
3. This Annex also sets out the FCA's view of how the proposed rules are compatible with the duty on the FCA to discharge its general functions (which include rule-making) in a way which promotes effective competition in the interests of consumers (section 1B(4)). This duty applies in so far as promoting competition is compatible with advancing the FCA's consumer protection and/or integrity objectives.
4. In addition, we have considered the recommendations made by the Treasury under s 1JA FSMA about aspects of the economic policy of His Majesty's Government to which we should have regard in connection with our general duties.
5. This Annex includes our assessment of the equality and diversity implications of these proposals.

The FCA's objectives and regulatory principles: Compatibility statement

6. 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.
7. 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.
8. 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.

9. 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 economic way

10. 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

11. As set out in Annex 2, we do not expect the proposals to result in significant costs and, accordingly, we have not undertaken a CBA.

The need to contribute towards achieving compliance by the Secretary of State with section 1 of the Climate Change Act 2008 (UK net zero emissions target) [and section 5 of the Environment Act 2021 (environmental targets)]

12. We have considered the environmental, social and governance (ESG) implications of our proposals, including our duty under sections 1B(5) and 3B(c) of FSMA to have regard to contributing towards the Secretary of State achieving compliance with the net-zero emissions target under section 1 of the Climate Change Act 2008 and environmental targets under section 5 of the Environment Act 2021. While we do not consider these proposals to be relevant to those targets, we welcome consultation feedback on any ESG implications.

The general principle that consumers should take responsibility for their decisions

13. 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 Guide and better guidance will result indirectly in better consumer outcomes and protection.

The responsibilities of senior management in relation to compliance with requirements imposed under FSMA, especially where they relate to consumers

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

The desirability of exercising our functions in a way that recognises the differences in the nature of - and objectives of - businesses carried on by different persons including mutual societies and other kinds of business organisation

15. 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 to advance our [operational and secondary] objectives

16. This consultation is aligned with these objectives. It is providing further information to firms subject to FSMA Financial Crime Rules.

The responsibilities of senior management

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

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

18. The consultation is aligned with this objective and provides transparent communication on our proposals to the firms we supervise.
19. In formulating these proposals, the FCA has had regard to 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).

Expected effect on mutual societies

20. The FCA does not expect the proposals in this paper to have a significantly different impact on mutual societies.

Compatibility with the duty to promote effective competition in the interests of consumers

21. In preparing the proposals as set out in this consultation, we have had regard to the FCA's duty to promote effective competition in the interests of consumers. This is set out in paragraphs 1.13 of the consultation paper.

Equality and diversity

22. 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.

Legislative and Regulatory Reform Act 2006 (LRRRA)

23. Under the Legislative and Regulatory Reform Act 2006 (LRRRA) the FCA is subject to requirements to have regard to a number of high-level 'Principles' in the exercise of some of our regulatory functions and to have regard to a 'Regulators' Code' when determining general policies and principles and giving general guidance (but not when exercising other legislative functions like making rules).
24. 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
25. 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 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.

- 26.** 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.
- 27.** 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.

Annex 4

Abbreviations used in this paper

Abbreviation	Description
AML	Anti-Money Laundering
APP	Authorised Push Payment
BaaS	Banking as a Service
CBA	Cost Benefit Analysis
CDD	Customer Due Diligence
COP	Confirmation of Payee
CTF	Counter Terrorist Financing
EDD	Enhanced Due Diligence
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 Customers
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
OFTI	The Office of Trade Sanctions Implementation
PSPs	Payment Service Providers
PF	Proliferation Financing

Appendix 1

Draft Handbook text

FINANCIAL CRIME GUIDE (AMENDMENT) INSTRUMENT 202X

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 (SI 2017/752); and
 - (3) regulation 60(1) (Guidance) of the Electronic Money Regulations 2011 (SI 2011/99).

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.

Notes

- D. In the Annex to this instrument, the notes (indicated by “**Note:**” or “*Editor’s note:*”) are included for the convenience of readers but do not form part of the legislative text.

Citation

- E. This instrument may be cited as the Financial Crime Guide (Amendment) Instrument 202X.

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, unless otherwise indicated.

1 Introduction

1.1 What is the FCG?

...

1.1.5 ...

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 authorised cryptoasset businesses firms and specified investment cryptoasset firms under the *Act*. *FCG 3* (Money laundering and terrorist financing) and *FCG 7* (Sanctions and proliferation finance), together with guidance in *SYSC* (particularly *SYSC 6*), will also be relevant to Annex 1 firms and cryptoasset firms registered with us under the *Money Laundering Regulations*.

...

1.1.9 *FCG* also contains guidance on how firms can meet the requirements of the *Money Laundering Regulations* and the ~~EU~~ Funds Transfer Regulation. While the relevant parts of the guide that refer to the *Money Laundering Regulations* may be 'relevant guidance' under these regulations, it is not approved by HM Treasury.

...

1.2 How to use the FCG

...

1.2.3 Firms should apply the guidance in a risk-based, proportionate way taking into account such factors as the nature, size and complexity of the firm. For example:

...

- ~~We say in *FCG 4.2.1G* (General — preventing losses from fraud) that it is good practice for firms to engage with relevant cross-industry efforts to combat fraud. A national retail bank is likely to have a greater exposure to fraud, and therefore to have more information to contribute to such~~

~~efforts, than a small local building society, and we would expect this to be reflected in their levels of engagement.~~

...

2 Financial crime systems and controls

2.1 Introduction

...

2.1.2 The Annex I *financial institutions* ~~and cryptoasset businesses which that~~ we supervise ~~for compliance with their obligations only~~ under the *Money Laundering Regulations* are not subject to the financial crime rules in *SYSC*. ~~But~~ However, the guidance in this chapter applies to them as it can assist them to comply with their obligations under the Regulations.

...

2.2 Themes

Governance

2.2.1 ...

Self-assessment questions:

...

- Is there evidence that **issues have been escalated** where warranted?

In banking as a service, embedded finance and similar delivery arrangements, firms should consider how financial crime responsibilities are allocated and overseen across the delivery chain. Where customer onboarding, payments activity or other operational services are performed by third parties, outsourced providers or other partners, regulated firms remain responsible for ensuring that appropriate financial crime systems and controls are maintained.

...

Management information (MI)

2.2.2 ...

MI may come from more than one source, for example the compliance department, internal audit, the MLRO or the nominated officer.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
----------------------------------	----------------------------------

• <u>Senior management review the content, quality and relevance of MI provided on an ongoing basis and provide appropriate challenge, as required.</u>	• <u>Data provided to senior management is of limited value and lacking sufficient detail and context to enable senior management to understand the financial crime risks to which their firm is exposed and make informed, risk-based decisions.</u>
---	---

Structure

2.2.3

...

Examples of good practice	Examples of poor practice
...	
• ~~A firm has considered how counter fraud and anti money laundering efforts can complement each other.~~	...
...	

Risk assessment

2.2.4

...

Examples of good practice	Examples of poor practice
...	
• The firm considers financial crime risk when designing new products and services.	
• <u>The firm continually assesses the risks posed by its customers, including dormant or inactive customers, keeps them under regular review, and has adequate, documented procedures for customer offboarding.</u>	

...

3 Money laundering and terrorist financing

3.1 Introduction

3.1.1 **Who should read this chapter?** This section applies to **all firms** ~~who~~ that are subject to the money laundering provisions in SYSC 3.2.6A – J or SYSC 6.3. It also applies to Annex I **financial institutions**, **cryptoasset businesses** and **e-money institutions** for ~~whom~~ which we are the supervisory authority under the *Money Laundering Regulations*.

...

3.1.7A ~~The European Supervisory Authorities (ESAs) have produced guidelines that firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. The *Money Laundering Regulations* require firms subject to the regulations to take account of these guidelines when complying with the customer due diligence requirements in Regulations 33 and 37. [deleted]~~

3.1.8 When considering a firm's systems and controls against money laundering and terrorist financing, we will consider whether the firm has followed relevant provisions of the JMLSG's guidance, and guidance issued by the *FCA* ~~or taken account of the ESA guidelines.~~

3.2 Themes

Governance

3.2.1 The guidance in FCG 2.2.1G on governance in relation to financial crime also applies to money laundering. We expect senior management to take responsibility for the firm's anti-money laundering (AML) measures. This includes ~~knowing about~~ understanding the money laundering risks to which the firm is exposed and ensuring that steps are taken to mitigate those risks effectively. Firms should develop a responsible approach to AML measures at the earliest stage of their growth journey, and ensure that governance, control and compliance frameworks evolve in step with increasing business complexity and scale.

...

...

Risk assessment

3.2.3 ...

Under section 188 of the Economic Crime and Corporate Transparency Act 2023, firms are able to share information with one another for the purpose of preventing, detecting and investigating economic crime. Regulated firms should use this information to assist with their risk-based decision making and

should not share it for commercial reasons or to provide sectors with additional ~~powers~~ means to exclude customers inappropriately. Firms must also consider their obligations under the *General data protection regulation*.

Firms assessing customers at onboarding should consider the risks attached to the sector from which their customer's source of wealth or funds has originated (regulation 18A (Risk assessment by relevant persons in relation to proliferation financing) of the *Money Laundering Regulations*).

When assessing the risks to which their business is subject, firms should consider the risks arising from the sector(s) in which their customers or business partners operate. Where a firm anticipates dealing with those whose source of wealth, or source of funds, derives from cryptoasset activities, it should consider factors including the jurisdiction the cryptoasset services the customer used operates in, as well as risk from anonymity, privacy, or decentralised products and services – for example, whether a customer has used a regulated cryptoasset entity in a low-risk jurisdiction or an unregulated entity in a high-risk jurisdiction.

Firms should consider, as part of their financial crime risk assessment and governance arrangements, whether data loss or cyber incidents could give rise to financial crime risks. This may include risks relating to fraud, identity theft, account takeover, data manipulation, misuse of customer or transactional information, or disruption to financial crime controls such as customer due diligence, sanctions screening, transaction monitoring and suspicious activity reporting. Where relevant and proportionate, firms should consider whether their response to such incidents would require additional financial crime monitoring, customer protection measures, regulatory notifications, evidence preservation or remediation of affected financial crime controls.

Self-assessment questions:

- Which parts of the business present **greater risks** of money laundering, terrorist financing and ~~PF~~ proliferation financing? (Has your firm identified the risks associated with different types of customers or beneficial owners, products, services, activities, transactions, business lines, geographical locations and delivery channels (e.g. internet, telephone, branches)? Has it assessed the extent to which these risks are likely to be an issue for the firm?)

...

- ~~For cryptoasset businesses, how do you assess and address the risks of different types of cryptoasset (e.g. anonymity enhanced or privacy coins)?~~
- In addition to the considerations above, for cryptoasset businesses, authorised cryptoasset firms or specified investment cryptoasset firms, how do you assess and address:
 - the risks of different types of cryptoassets to which your firm is exposed; and
 - whether your business model is exposed to risks from particular products and services, such as anonymity or privacy coins, mixers or

tumblers, or activities with a high degree of decentralisation or automation, or without an obvious intermediary?

- How do you assess and address any risks arising from customers engaging in unregulated activities, particularly where those activities are conducted from, or involve, countries whose regulation of cryptoasset activities differs from that of the UK?

Examples of good practice	Examples of poor practice
...	
...	• A UK branch or subsidiary relies on group risk assessments without assessing their compliance with UK AML requirements.
• The firm engages with public-private partnerships and private-private partnerships to gather insights on the latest financial crime typologies and additional controls that might be relevant and shares its own best practice examples.	• <u>A manager is active in private markets but has no formal Ultimate Beneficial Owner verification process for multi-layered or offshore structures.</u>
• <u>The firm's customer records clearly document, explain and evidence how the risk assessment has informed the application of relevant controls to the business relationship, and to individual transactions, enabling the firm to demonstrate compliance with its obligations.</u>	• <u>A manager is active in private markets, but its risk assessments do not adequately cover financial crime risk.</u>
	• <u>A manager outsources CDD/EDD processes without maintaining oversight and monitoring, thus failing to meet obligations under the Money Laundering Regulations.</u>

See ~~regulation~~ regulations 18 and 18A of the *Money Laundering Regulations*, SYSC 3.2.6AR, SYSC 3.2.6CR, SYSC 6.3.1R and SYSC 6.3.3R.

Customer due diligence (CDD) checks

3.2.4

...

Firms are required to collect proof of company registration (or an excerpt from the register) before establishing a business relationship with certain legal entities including a company subject to the requirements of Part 21A of the Companies Act 2006, a limited liability partnership or an eligible Scottish partnership. Firms are required to report to Companies House material discrepancies between this information and information which otherwise becomes available to them in the course of complying with the *Money Laundering Regulations*. Firms may wish to refer to further guidance from ~~the~~ Companies House. Firms only need to report to Companies House in case of a material discrepancy. Schedule 3AZA (Material Discrepancies) of the *Money Laundering Regulations* defines a material discrepancy.

Where a firm provides a customer with a pooled client account, it should have regard to the requirements in regulation 29 (Additional customer due diligence measures: credit institutions and financial institutions) of the *Money Laundering Regulations*, including taking the steps set out in regulation 29(11) to (17), where applicable.

Specific CDD requirements apply where a customer opening an account is an insolvent banking customer. Firms should have regard to regulation 30ZA (Insolvent bank customers) of the *Money Laundering Regulations*.

...

Firms should note that ~~an~~ electronic identification ~~process~~ tools and the use of digital identity solutions may be regarded as a reliable ~~source~~ sources for the purposes of CDD verification where ~~that process is~~ they are independent of the person whose identity is being verified, secure ~~from~~ against fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person ~~with that identity~~. Firms using digital identities as part of their CDD should have regard to the government's [guidance on using digital identities](#) under the *Money Laundering Regulations*.

A UK-authorised stablecoin issuer, or a third party carrying out the AML checks on its behalf, should conduct CDD checks within a reasonable timeframe during onboarding and redemption, while ensuring compliance with its obligations under regulations 27 (Customer due diligence) and 28 (Customer due diligence measures) of the *Money Laundering Regulations*. Redemption should only occur once relevant financial crime obligations have been complied with.

Authorised cryptoasset firms and cryptoasset businesses should also consider how technology can be used, where appropriate, to support CDD, EDD and ongoing monitoring, such as to identify cloned documentation, identify engagement with higher risk products and/or services, and otherwise enable them to fulfil their financial crime obligations.

Where a firm uses third-party tools or services to support key elements of its CDD or transaction monitoring processes, it remains responsible for ensuring that appropriate oversight and governance arrangements are in place to ensure that regulatory requirements and responsibilities are met.

Firms should ensure that they are mindful of the requirement to keep copies of any documents and information obtained to meet CDD requirements.

Self-assessment questions:

...

- With **non-face-to-face** transactions, how does your firm's approach provide confidence that the person is **who they claim to be**? How do you test any technology used as part of onboarding, including for authorised cryptoasset firms and cryptoasset businesses?

Examples of good practice	Examples of poor practice
...	
• The firm understands and documents the ownership and control structures (including the reasons for any complex or opaque corporate structures) of customers and their beneficial owners.	• The firm allows language difficulties or customer objections to get in the way of proper questioning to obtain necessary CDD information.
• <u>The firm has appropriate service level agreements in place with third-party providers, reviews the quality and appropriateness of tools and services provided on a regular basis and ensures that ongoing regulatory requirements and responsibilities are met.</u>	• <u>The firm uses a third-party tool to conduct adverse news screening as part of their CDD programme but has not assessed the applicability and validity of the data sources used.</u>
...	
• Staff who approve new or ongoing business relationships satisfy themselves that the firm has obtained adequate CDD information before doing so.	...
• <u>A firm utilises technology, such as blockchain analytics, when completing source of funds checks, allowing them to identify risks such as privacy enhancing coins.</u>	...

See regulations 5, 6, 27, 28, 30A, 31, 33, 34 and 35 of the *Money Laundering Regulations*.

Ongoing monitoring

3.2.5

...

Examples of good practice	Examples of poor practice
...	
...	The firm's measures fail to conduct a full assessment of the risk. For instance, the firm does not consider changes in the nature of the relationship or expected activities.
...	<u>The firm makes no use of data or blockchain analytics in its ongoing monitoring procedures (and does not compare information obtained to that available from original or refreshed CDD and EDD) to complete its existing processes when cryptoasset activities are identified.</u>
...	<u>The firm utilises third-party technology as part of its relevant control framework and is unable to explain or evidence the basis for findings made or scoring applied.</u>
The firm updates CDD information and reassesses the risk associated with the business relationship where monitoring indicates material changes to a customer's profile.	<u>A firm engaging in cryptoasset activities deploys a rigid rule concerning the number of 'hops' or relevant transfers it scrutinises when undertaking due diligence on its customers and/or relevant transactions, which does not account for risk-appropriate measures.</u>
<u>The firm engages with and calibrates tools employed to reflect the risks identified in its business, and documents audit trails for all rules and decisions</u>	<u>A manager has no formal transaction monitoring process.</u>

<u>within the relevant control framework.</u>	
• <u>A firm conducting cryptoasset activities makes proactive use of on-chain monitoring tools to allow it to identify higher risk activities such as irregular patterns of cryptoasset transactions both within the cryptoasset ecosystem and off-ramping to other financial service sectors.</u>	

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

...

Source of wealth and source of funds

- 3.2.6 Establishing the source of funds and the source of wealth ~~can be useful~~ is important for ongoing monitoring and due diligence purposes because it can help firms ascertain whether the level and type of transaction is consistent with the firm's knowledge of the customer. It is a requirement where the customer is a PEP.

...

[~~Editor's Note: see <https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering>~~ FG25/3: Treatment of politically exposed persons.]

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 from a third country (see regulation 34 of the *Money Laundering Regulations*), 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. Regulation 34A (Enhanced customer due diligence: cryptoasset exchange providers, custodian wallet providers and correspondent relationships) of the *Money Laundering Regulations* contains the same requirements for cryptoasset businesses.

JMLSG guidance sets out how firms should apply EDD in differing correspondent trading relationships.

- **Politically exposed persons (PEPs), family members and known close associates of a PEP:** a PEP is a person entrusted with a prominent public function, other than as a middle-ranking or more junior official. PEPs (as well as their family members and known close associates) must be subject to enhanced scrutiny. A senior manager at an appropriate level of authority must also approve the initiation of a business relationship with a PEP (or with a family member, or known close associate, of a PEP). This includes approving a relationship continuing with an existing customer who became a PEP after the relationship begun. In meeting these obligations firms may have regard to the *FCA's* guidance on a risk-based approach to PEPs. Regulation 35(3A) (Enhanced customer due diligence: politically exposed persons) of the *Money Laundering Regulations* also provides that the starting point for the risk assessment is that a domestic PEP, or a family member or known close associate of a domestic PEP, presents a lower level of risk than a non-domestic PEP.
- **Business relationships or a 'relevant transaction' where either party is established in a ~~high-risk third country~~ FATF call for action country:** the *Money Laundering Regulations* ~~defines~~ define:
 - (a) a high-risk third country as a country named ~~by FATF on its~~ in FATF's list of High-Risk Jurisdictions subject to a Call for Action ~~or its list of Jurisdictions under Increased Monitoring~~;
 - ...
 - ...
- **Other transactions:** EDD must be performed:
 - (a) ~~in any case~~ where a transaction is unusually complex or unusually large (having regard to the nature of the transaction), or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose. In this scenario, there are specified EDD measures which must include, as far as reasonably possible, examining the background and purpose of the transaction and increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appears to be suspicious;
 - (b) ...
 - (c) where findings from blockchain analysis indicates exposure to criminal or sanctioned activities. In these circumstances, firms should consider how their AML policies, controls and procedures should be strengthened where they are exposed to non-UK-issued qualifying stablecoins, particularly where the regulatory treatment of those stablecoins differs from that in the UK.
 - ...

Handling higher risk situations – enhanced due diligence (EDD)

3.2.8

...

Examples of good practice	Examples of poor practice
...	Senior management do not give approval for taking on high risk customers. If the customer is a PEP or a ~~non-EEA~~ <u>non-UK</u> correspondent bank, this breaches the <i>Money Laundering Regulations</i>.
...	
A correspondent bank gathers information about respondent banks' procedures for sanctions screening, PEP identification and management, account monitoring and suspicious activity reporting.	...
<u>A firm engaging in cryptoasset activities or with cryptoassets considers when customers or transactions involving cryptoasset activities may present a higher risk of money laundering or terrorist financing, and applies enhanced due diligence as appropriate, including customers or transactions funded by unhosted wallets, or where other privacy enhancing measures are used such as mixers, tumblers or privacy-enhancing coins.</u>	...

• <u>A firm engaging in cryptoasset activities uses blockchain analytics to complement existing risk-based anti-money laundering policies and procedures to allow early and timely identification and flag any connections to anonymity-enhancing technology such as privacy layers, tumblers or mixers.</u>	
• <u>A firm applies EDD for transactions involving unhosted wallets.</u>	

See regulations 33, 34, 34(1)(d), 35 and 35(5)(a) of the *Money Laundering Regulations*.

...

Liaison with law enforcement

3.2.10

...

Staff must report their concerns and may do so to the firm's nominated officer, who must then consider whether a report to NCA is necessary based on all the information at their disposal. Law enforcement agencies may seek information from the firm about a customer, often through the use of ~~Production~~ Investigative Court Orders (see *FCG Annex 1*).

Firms may engage with, and provide assistance to, other bodies for legitimate public interest purposes, including supporting law enforcement and safeguarding the UK's national security. Firms should establish and maintain appropriate working relationships with law enforcement agencies and other relevant authorities where this assists those purposes. Where appropriate, firms should provide advice and support relevant to the particular circumstances.

Self-assessment questions:

...

- Are reporting procedures clear to staff?
- Do staff report suspicions to the **nominated officer**? If not, does the nominated officer take steps to identify understand why reports are not being made? How does the nominated officer deal with reports received?
- What evidence is there of the rationale **underpinning decisions** about whether a SAR is justified or not made to law enforcement?

- Is there a documented process for responding to **Production Investigative Court Orders**, with clear timetables?
- Can your firm retrieve records promptly in response to an Investigative Court Order?
- Are staff and relevant procedures clear about key differences between ‘Defence Against Money Laundering Suspicious Activity Reports’ under the Proceeds of Crime Act 2002, and ‘Defences Against Terrorist Financing’ under the Terrorism Act 2000, regarding thresholds and exemptions?

Examples of good practice	Examples of poor practice
...	
...	• A firm provides extraneous and irrelevant detail in response to a Production an Investigative Court Order.

See regulation 21 of the *Money Laundering Regulations* and s.330 POCA and s.331 POCA and s.21A of the Terrorism Act 2000.

Record keeping and reliance on others

3.2.11 ...

Self-assessment questions:

- Can your firm retrieve records **promptly** in response to a ~~Production~~ an Investigative Court Order?

...

...

Customer payments

3.2.13 This section applies to ~~banks~~ payment service providers and cryptoasset businesses subject to SYSC 6.3.

...

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, authorised cryptoasset firms and specified investment cryptoasset firms in implementing this requirement but they should also have regard to specific expectations set out by the *FCA*. ~~For further information, see www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule~~ Firms are reminded of their obligations

under the ‘Travel Rule’, which includes collecting, verifying and transmitting information regarding the originator and beneficiary for cryptoasset transfers.

Where required information is incomplete or missing, firms should establish a process for requesting information from counterparties and making a risk-based decision on what to do with a transaction if the required information cannot be obtained. Firms are reminded of their requirement to report persistent failure to comply with the Travel Rule to the FCA.

For further information, see ‘FCA sets out expectations for UK cryptoasset businesses complying with the 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.->]~~

If payment service providers (PSPs) identify another PSP as repeatedly failing to provide required information (eg, the payer’s name) the FCA should be notified by email to repeatedlyfailingpsp@fca.org.uk.

Examples of good practice	Examples of poor practice
...	
• ~~An intermediary bank chases up missing information. A bank identifies other payment service providers that repeatedly fail to provide the required information with payments and reports this to the FCA.~~	...
...	

...

3.4 Sources of further information

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

- The *Money Laundering Regulations*
- The ~~NCA's website~~ [NCA's website](#), which contains information on how to report suspicions of money laundering: ~~www.nationalcrimeagency.gov.uk~~
- The latest UK National Risk Assessment of money laundering and terrorist financing 2020 – ~~www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020~~ [UK National Risk Assessment of money laundering and terrorist financing 2025](#)
- The JMLSG's guidance on measures firms can take to meet their anti-money laundering obligations, which is available from its ~~website: www.jmlsg.org.uk.~~ [website](#)
- ~~The government's~~ [guidance on using digital identities with the Money Laundering Regulations](#)

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

- Material relevant to terrorist financing that can be found throughout the JMLSG guidance: [www.jmlsg.org.uk JMLSG guidance](#)
- ~~The European Supervisory Authorities (ESAs) have published risk factors guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849-
https://www.esa.europa.eu/sites/default/files/documents/10180/1890686/66ec16d9-0e02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20%28JC%202017%2037%29.pdf~~
- FATF's work on terrorist financing: <http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html> [terrorist financing](#)

3.4.3 To find out more on customer payments, see:

- ~~JMLSG guidance (www.jmlsg.org.uk/guidance/current-guidance/)~~ [JMLSG guidance](#):
 - ~~Sector 22 of Part II (Cryptoasset exchange providers and custodian wallet providers) and Annex 22-I of Part II (Cryptoassets Transfers ('Travel Rule'));~~ and
 - ~~Chapter 1 of Part III (Transparency in electronic payments (Wire transfers)), which will be banks' chief source of guidance on this topic.~~
- ~~The Basel Committee's May 2009 paper on due diligence for cover payment messages: www.bis.org/publ/bcbs154.pdf~~
- The Wolfsberg Group's statement on payment standards: <https://db.wolfsberggroup.org/assets/373dbb28-b518-4080-82cc4be7a54aa16e/Wolfsberg%20Group%20Payment%20Transparency%20Standards%20-2023.pdf> [statement on payment standards](#)
- The *Money Laundering Regulations*

- ~~FCA statement: www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule~~ [FCA statement on cryptoasset travel rule](#)
- [FCA guidance on payment service providers](#)

...

4 Fraud

4.1 Introduction

...

4.1.3 The contents of *FCG*'s fraud chapter reflect the *FSA*'s previous thematic work in this area, as well as the *FCA*'s publications in relation to authorised push payment (APP) fraud and money mule activity. This means it does not specifically address such topics as ~~plastic card~~ unauthorised fraud, cheque or insurance fraud. This is not because the *FCA* regards fraud prevention of these topics as unimportant. Rather it reflects ~~our view that our limited resources are better directed elsewhere, given the strong incentive firms should have to protect themselves from fraud; and the number of other bodies active in fraud prevention. Links to some of these other bodies are provided in FCG 4.4.~~ the existing incentives and liability protections in place for certain types of fraud, as well as the extensive landscape of policies and initiatives designed to incentivise and support firms to improve their detection and prevention of fraud. This guidance supports the cross-system approach required to tackle fraud and reflects that our resources have been directed towards topics such as APP fraud (including investment fraud) and money mule activity.

4.1.4 The Failure to Prevent Fraud offence was introduced as part of the Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023) and came into force on 1 September 2025. Under ECCTA 2023, an organisation may be criminally liable where an employee, agent, subsidiary undertaking or other 'associated person' commits a fraud intending to benefit the organisation and the organisation did not have reasonable fraud prevention procedures in place. The Home Office has issued guidance to organisations, which is supported by sector-specific guidance published by UK Finance.

The *FCA* does not enforce or give guidance on the Failure to Prevent Fraud Offence under ECCTA 2023. But:

- firms which are subject to SYSC 3.2.6R and SYSC 6.1.1R are under a separate regulatory obligation to establish and maintain effective systems and controls to mitigate financial crime risk. A breach of the Failure to Prevent Fraud Offence may impact upon a firm's compliance with these SYSC rules; and
- e-money institutions and payment institutions must satisfy us that they have robust governance, effective risk procedures and adequate internal control mechanisms. See regulation 6 of the *Electronic Money Regulations* and regulation 6 of the *Payment Services Regulations*.

4.2 Themes

Preventing losses from fraud

- 4.2.1 All firms will wish to protect themselves and their customers from fraud. Management oversight, risk assessment and fraud data will aid this, as will tailored controls on the ground. We expect a firm to consider the full implications of the breadth of fraud risks it faces, including the risk that it is used to move the proceeds of fraud, which may have wider effects on its reputation, its customers and the markets in which it operates.

~~The general guidance in FCG 2 also applies in relation to fraud.~~

We expect a firm to place sufficient focus on ensuring customers do not become victims of fraud and that the firm is not being exploited by fraudsters to move the proceeds of fraud.

The topics outlined in FCG 4.2 provide detail on our expectations for firms' anti-fraud prevention systems and controls. In addition to the guidance set out in this section, firms should consider how the self-assessment questions and good and poor practice examples set out FCG 2.2 (Themes) can be applied to fraud.

...

Examples of good practice	Examples of poor practice
• The firm takes a view on what areas of the firm are most vulnerable to fraudsters, and tailors defences accordingly	• Senior management appear unaware of fraud incidents and trends. No management information is produced.
• Controls adapt to new fraud threats.	• Fraud losses are buried in bad debts or other losses.
• The firm engages with relevant cross-industry efforts to combat fraud (e.g. data-sharing initiatives like CIFAS and the Insurance Fraud Bureau, collaboration to strengthen payment systems, etc.) in relation to both internal and external fraud.	• There is no clear and consistent definition of fraud across the business, so reporting is haphazard.
• Fraud response plans and investigation procedures set out how the firm will respond to incidents of fraud.	• Fraud risks are not explored when new products and delivery channels are developed.
• Lessons are learnt from incidents of fraud.	• Staff lack awareness of what constitutes fraudulent behaviour

	(e.g. for a salesman to misreport a customer's salary to secure a loan would be fraud).
• ~~Anti-fraud good practice is shared widely within the firm.~~	• ~~Sales incentives~~ act to encourage staff or management to turn a blind eye to potential fraud.
• To guard against insider fraud, staff in high risk positions (e.g. finance department, trading floor) are subject to enhanced vetting and closer scrutiny. 'Four eyes' procedures (see <i>FCG Annex 1</i> for common terms) are in place.	• Banks fail to implement the requirements of the Payment Services Regulations and Banking Conduct of Business rules, leaving customers out of pocket after fraudulent transactions are made.
• ~~Enhanced due diligence~~ is performed on higher risk customers (e.g. commercial customers with limited financial history. See 'long firm fraud' in <i>FCG Annex 1</i>).	• ~~Remuneration structures~~ may incentivise behaviour that increases the risk of mortgage fraud.
• ~~Cryptoasset businesses pre-screen~~ outbound transactions for addresses linked to fraud.	

Governance

4.2.1A

We expect **senior management** to take **clear responsibility** for managing fraud risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management is actively engaged in the firm's approach to managing fraud risks that affect the firm and its customers, alongside its wider financial crime risks.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
• <u>The firm has a strategy for managing fraud risks, including a focus on protecting customers from the harms of fraud.</u>	• <u>There is no meaningful record or evidence of senior management considering fraud-specific risks as part of a wider financial crime strategy.</u>
• <u>The firm's strategy for managing fraud risks considers wider requirements, including those in the <i>Payment Services</i></u>	

<i>Regulations, the Electronic Money Regulations and BCOBS.</i>	
---	--

Management information (MI)

4.2.1B

MI should provide senior management with **sufficient information** to understand the fraud risks to which their firm is exposed. MI should be provided regularly and ad hoc, to help senior management adhere to its own fraud risk appetite, to effectively manage fraud risks and to improve systems and controls.

Examples of fraud MI can include but are not limited to:

- rates of fraud detected;
- rates of fraud prevented;
- rates of false positive fraud alerts detected;
- the volumes and value of fraud losses;
- fraud alert handling times;
- root cause analysis of operational or process failures, gaps in onboarding or monitoring controls, and data quality issues;
- key trends, including fraud typologies being exploited by criminals, customer vulnerability and customer behaviour; and
- information from customers on the enabling tech and telecommunication platforms used in a fraud incident.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
• <u>The firm uses a clear and consistent definition of fraud across the business.</u>	• <u>Senior management appear unaware of fraud incidents or trends, caused by a lack of fraud MI being produced.</u>
• <u>MI is subject to regular review and analysis by appropriate teams, with clear escalation processes in place to ensure that significant risks or adverse trends are promptly brought to the attention of senior management and relevant risk functions.</u>	

Structure

4.2.1C

Firms' **organisational structures** to combat financial crime, including fraud, may differ. There is no one 'right answer' but the firms' structures should

promote coordination and information-sharing across the business in relation to fraud.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
<u>The firm has considered how anti-fraud and anti-money laundering efforts can complement each other.</u>	<u>The structure leads to a siloed anti-fraud approach, limiting coordination and information sharing across the firm's financial crime structures.</u>

Risk assessment

4.2.1D

A thorough understanding of its financial crime risks is key if a firm is to apply proportionate and effective systems and controls. Firms should identify and assess the fraud risks to which it is exposed. We expect a firm to consider the full implications of the breadth of fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

FCG 2.2.4 sets out our expectations on business-wide risk assessments for financial crime.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
<u>The firm takes a view on what areas of the firm are most vulnerable to fraudsters, and tailors defences accordingly. This could include fraud risks in products, services, delivery channels and customer journeys.</u>	<u>The firm fails to identify new or emerging fraud risks, limiting its ability to adapt systems and controls in response.</u>
<u>The firm considers the risk associated with various fraud types and typologies (eg, investment fraud as an APP fraud typology), when assessing the fraud risks.</u>	<u>The firm fails to consider fraud risks when new products and delivery channels are developed.</u>
<u>The firm can evidence the findings of risk assessments and evidence what actions were taken in response, to help protect customers from becoming the victim of fraud.</u>	

Policies and procedures

- 4.2.1E FCG 2.2.5 sets out our expectation that a firm must have in place up-to-date policies and procedures appropriate to its business which should be **readily accessible, effective** and **understood** by all relevant staff. We expect these policies and procedures to include the firm's arrangements for managing the potential harms arising from its fraud risks.

Staff recruitment, vetting, training, awareness and remuneration

- 4.2.1F FCG 2.2.6 sets out our expectations in relation to recruitment, vetting, training, awareness and remuneration. In line with these expectations, firms should ensure that the staff they employ in fraud-specific roles possess the skills, knowledge and expertise to carry out their functions effectively. We expect all employees to receive regular fraud training to ensure staff at all levels are aware of the role they play in fraud prevention.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
• <u>Anti-fraud good practice is shared widely within the firm.</u>	• <u>Employees do not receive appropriate training to equip them to identify suspicious behaviours in relation to fraud.</u>
• <u>Employees in fraud-specific roles receive more specific and focused training.</u>	• <u>Sales incentives act to encourage staff or management to turn a blind eye to potential fraud.</u>
• <u>To guard against insider fraud, staff in high-risk positions (eg, the finance department or trading floor) are subject to enhanced vetting and closer scrutiny. 'Four eyes' procedures (see <i>FCG</i> Annex 1 for common terms) are in place.</u>	• <u>Remuneration structures may incentivise behaviour that increases the risk of mortgage fraud.</u>

Quality of oversight

- 4.2.1G FCG 2.2.7 sets out that a firm's efforts to combat financial crime should be subject to **challenge** and we expect senior management to ensure that policies and procedures are appropriate and followed.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
---	---

Internal audit and compliance are routinely testing the firm's fraud defences as part of its wider financial crime testing.	Compliance and internal audit teams lack experience in fraud-specific matters.
---	--

Customer treatment

4.2.1H

We expect firms to have appropriate systems and controls in place to ensure they are engaging with customers appropriately in relation to fraud, including:

- ensuring that customers have easily accessible routes for reporting instances of fraud, as well as suspicions of fraud;
- ensuring they consider customer vulnerability;
- ensuring that legal obligations in relation to reimbursement are met;
- ensuring that appropriate support is provided to customers that have been victims of fraud; and
- ensuring that customers have accessible routes for raising complaints in relation to fraud.

These systems and controls should support the firms' obligations under the Consumer Duty in relation to the standard of care they should be providing to customers.

<u>Examples of good practice</u>	<u>Examples of poor practice</u>
Teams are adequately resourced to respond to customer queries in relation to fraud, helping ensure they can take prompt action to prevent fraud and recover funds where appropriate.	Firms do not test their internal responses to fraud reports (or reports on suspicions of fraud), leading to slow or inadequate responses going unchecked.
The firm's routes for reporting fraud (or suspicions of fraud) are easily accessible, consistent across all levels and types of customers, and responded to promptly.	Firms rely on passive anti-fraud messaging and content.
Firms engage with customers to raise awareness of fraud risks to help empower customers to better protect themselves from becoming victims of fraud.	Firms' responses to complaints are insufficiently tailored to the specific case.

• <u>The firm's complaints handling process ensures that the customer has clear channels to raise complaints and that they receive regular communication throughout the process.</u>	• <u>Firms offboard victims of fraud rather than exploring other proportionate and risk-based alternatives, such as enhanced monitoring, tailored controls or targeted support.</u>
--	---

APP fraud and money mules

4.2.1I

FCG 4.2.1I to FCG 4.2.1L set out our expectations for onboarding, monitoring and reporting, through the lens of tackling APP fraud and money mules. To support the general themes for fraud systems and controls (set out in FCG 4.2), firms should consider whether the guidance and good practice examples set out below can be also applied to other fraud types.

APP fraud

APP fraud is where a victim is deceived into authorising a payment either:

- to an account that they think belongs to a legitimate payee but is actually controlled by a fraudster; or
- for something they believed was legitimate but is actually fraudulent.

APP fraud has significant financial consequences for victims and undermines security and trust in the UK economy. The FCA's guidance on APP fraud aims to support the efforts across the wider system to tackle APP fraud, including:

- **Confirmation of Payee (CoP)** – the name-checking service designed to reduce APP fraud and misdirected payments. Firms are required to implement API solutions to connect with Pay.UK's central CoP directory. It covers 99% of Faster Payments and CHAPS transactions in the UK.
- **Payment Services Regulations 2017** – payment service providers (PSPs) can slow down the processing of outbound APP transactions where they have reasonable grounds to suspect fraud or dishonesty on the part of someone other than the payer.
- **APP scams reimbursement requirement** – requires sending firms to reimburse in-scope APP scams reported by their customers, within 5 or (in exceptional circumstances) 35 business days, with limited exceptions. The sending firm can claim 50% of the cost of reimbursement from the receiving firm, with a maximum reimbursement limit of up to £85,000 per APP scam claim. The requirement applies for both Faster Payments and CHAPS transactions sent and received in the UK.

APP fraud typologies

There are various fraud typologies within APP fraud, including purchase scams, advanced fee fraud and romance fraud. Another key typology is investment fraud, which typically involves misappropriation of funds or fraud by deception, and which may be facilitated through opaque investment structures, unauthorised collective investment schemes or Ponzi schemes.

We expect firms to consider the risks of different APP fraud typologies, including investment fraud, as part of their anti-fraud systems and controls.

Money mules

Money muling is a money-laundering technique where criminals use ‘money mule’ bank accounts to store and transfer criminal funds. A ‘money mule’ is recruited by criminals to move the criminal funds, either knowingly or unknowingly. Where an individual is an unknowingly involved money mule, they will often have been deceived by fraudsters, who present seemingly legitimate opportunities or plausible explanations to recruit individuals.

Money mule networks play a significant role in both enabling fraud and facilitating the movement and cashing-out of the proceeds of fraud.

Onboarding

4.2.1J FCG 3.2.4 sets out our expectations in relation to customer due diligence (CDD) checks. Firms must **identify** their customers and understand the **purpose** and **intended nature** of the customer’s relationship with the firm. Firms must collect information about the customer, which should be sufficient to obtain a complete picture of the risk associated with the business relationship and provide a meaningful basis for subsequent monitoring.

We expect firms to take proactive steps to consider the types of checks that will help mitigate the fraud risks relevant to their customers, as well as the risks associated with receiving and moving the proceeds of fraud (money muling). Firms should consider the types of onboarding checks that will create a holistic view of the customer to provide a meaningful basis to support the firm’s approach to fraud risk management and subsequent fraud monitoring. Firms should take steps to update their understanding of the customer and any associated risks throughout the lifecycle of the customer relationship.

<u>APP fraud</u>	
<u>Examples of good practice</u>	<u>Examples of poor practice</u>
<u>Sufficient onboarding checks are undertaken to build a holistic view of the customer to help determine whether there is an increased risk that the customer could become a victim of APP fraud. A firm identifies a range of information sources to assist with behavioural profiling.</u> <u>Customer profile indicators</u> <u>age;</u> <u>employment status;</u>	<u>Firms fail to keep accurate records of information gathered during onboarding checks.</u>

• <u>salary/income sources; and</u> • <u>expected account turnover.</u> <u>Digital profile indicators</u> • <u>device identifiers;</u> • <u>IP addresses;</u> • <u>geolocation data; and</u> • <u>biometrics.</u>	
• <u>The firm has processes in place for utilising industry-led fraud databases to conduct additional fraud checks as part of its wider customer due diligence processes. These processes include acting upon information gathered as part of these checks.</u>	• <u>The firm undertakes basic onboarding checks that are not kept up to date or do not inform the holistic view of the customer. The firm relies solely on transaction monitoring to identify potential fraud red flags.</u>
• <u>Where there is reasonable opportunity to do so, the firm identifies customer vulnerability and assesses whether these vulnerabilities could lead to an increased risk of the customer becoming a victim of APP fraud, both at onboarding and throughout the customer relationship.</u>	• <u>Firms do not take steps to satisfy themselves as to how the data held on fraud databases can help inform their approach to fraud-related onboarding checks.</u>
• <u>The firm implements effective checks for identifying synthetic or counterfeit documentation.</u>	• <u>Firms are only aware of customer vulnerabilities after a fraud has occurred.</u>

<u>Money mules</u>	
<u>Examples of good practice</u>	<u>Examples of poor practice</u>
• <u>Sufficient onboarding checks are undertaken to build a holistic view of the customer to help determine whether there is an increased risk that the customer could be a money mule and inform the subsequent monitoring of mule activity. This can include but is not limited to the following.</u>	• <u>The firm undertakes sufficient onboarding checks to build a holistic view of the customer but does not use this information to inform an assessment of money mule risk as part of its wider fraud risk management approach.</u>

<u>Customer profile indicators</u> • <u>age;</u> • <u>gender;</u> • <u>location;</u> • <u>employment status;</u> • <u>salary/income sources; and</u> • <u>expected account turnover.</u> <u>Digital profile indicators</u> • <u>device identifiers;</u> • <u>IP addresses;</u> • <u>geolocation data; and</u> • <u>biometric data</u>	
• <u>The firm has processes in place for using industry-led fraud databases to identify risks associated with money mule activity at onboarding and on an ongoing basis. These processes include acting upon information gathered as part of these checks.</u>	• <u>The firm undertook too few checks at onboarding to gain a full understanding of expected customer behaviour, leading to a potential increase in false positive transaction monitoring alerts or unnecessary investigations.</u>
	• <u>The firm applies a blanket approach to declining business based on the identification of historic markers in industry-led fraud databases, without considering the wider context of the customer's profile.</u>

Monitoring

4.2.1K

FCG 3.2.5 sets out that a firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. This means **scrutinising transactions and behaviour** to ensure that they are consistent with what the firm knows about the customer. Swift and proactive detection of unusual activity helps firms identify weaknesses in controls for detecting and preventing fraud and identifying money mule activity, as well as helping to identify emerging patterns in customer or fraudster behaviour, before they can be more widely exploited.

A firm should determine what represents suspicious activity for APP fraud, and relevant APP fraud typologies, based on the risks associated with its

business and customer base. Red flags for suspicious activity include, but are not limited to:

- changes in behavioural biometrics that are not aligned to the firm's understanding of the customer's expected behaviour;
- changes in expected turnover of account (eg, an increase in transactions or payment amounts);
- negative Confirmation of Payee (CoP) results;
- creation of new payees with high value transactions;
- customers seeking funds from various sources (eg, loans, borrowing from friends or family, liquidating assets);
- prompt dispersal of funds from a receiving account;
- sudden changes in personal circumstances; and
- customers using increasingly desperate tones in communications.

A firm should consider its fraud risks when developing systems and controls to allow for risk-based monitoring across all complexity levels and ensure there is sufficient focus on both inbound and outbound transaction monitoring. These systems and controls should be kept under regular review to ensure they remain aligned to the firm's fraud risks. Where alerts arise during monitoring, we expect firms to have adequate resource in place for fraud investigations to ensure the quality and speed of customer service is not negatively impacted. We also expect firms to keep comprehensive records of any subsequent investigations to ensure there is a clear evidential basis for objective decision making.

Having effective monitoring systems and controls in place to swiftly detect unusual activity will assist a firm's ability to deploy appropriate frictions to help prevent APP fraud. We expect firms to consider appropriate warnings for customers and deploy these at appropriate points throughout the payment journey, to help prevent customers falling victim to APP fraud.

Ongoing monitoring is an important tool in detecting and disrupting money mule activity. We expect firms to have systems and controls in place to analyse the flow of funds, to help identify and disrupt mule activity originating from different fraud types, as well as help detect further account holders who may have received funds associated with mule activity, helping stop mule networks.

Firms should consider which money mule indicators are relevant to their business and customer base. Money mule indicators include, but are not limited to:

- unexpected or unexplained deposits into accounts;
- changes in expected account turnover;
- rapid dispersal of funds through networks of accounts (often within minutes of receipt);
- movement of funds to international jurisdictions;

- rapid withdrawal of funds from ATMs;
- changes in dormant accounts;
- online banking credentials changing; and
- the registration of new devices or changes to contact details that are not aligned to the firm's knowledge of the customer (potentially indicating that accounts have been sold after opening).

<u>APP fraud</u>	
<u>Examples of good practice</u>	<u>Examples of poor practice</u>
• <u>The firm undertakes transaction monitoring on inbound and outbound transactions to help identify unusual activity or transaction patterns, to help identify and prevent fraudulent transactions.</u>	• <u>Firms fail to use their fraud strategy, risk appetite or onboarding information to determine appropriate transaction monitoring thresholds.</u>
• <u>Transaction monitoring rules (dynamic or static) are developed by staff with appropriate expertise in fraud typologies most relevant to the firm. The rules are developed using the holistic customer information obtained at onboarding and are built to detect potential red flags.</u>	• <u>Staff are not adequately trained to understand potential red flags associated with customer behaviour or social engineering tactics by fraudsters, and how these can be associated with APP fraud.</u>
• <u>Where machine learning tools are used, a firm ensures they are used in a way that is proportionate to the size and complexity of its business. Key staff understand how the tools work to ensure transactions are monitored effectively and that the tools are tailored to the firm's needs.</u>	• <u>The firm relies solely on machine learning tools with limited understanding of how they work. These tools are not used in conjunction with other systems and controls, including effective onboarding checks and monitoring of behavioural biometrics.</u>
• <u>The firm regularly reviews and tests transaction monitoring alerts to ensure that trigger thresholds remain appropriate and fit for purpose.</u>	• <u>The firm fails to implement new transaction monitoring alerts in response to changing thresholds in a timely manner, limiting its ability to respond to immediate threats.</u>
• <u>The firm's controls include deferrals to manual reviews</u>	• <u>Staff are not adequately trained to understand the rationale behind</u>

<u>where transaction monitoring alerts breach the firm's fraud thresholds.</u>	<u>transaction monitoring alerts or recognise red flags.</u>
• <u>Fraud alerts (including from transaction monitoring, customer contact, intel from other organisations) are investigated by suitably trained staff and appropriate interventions are deployed. These could include but are not limited to proactive engagement with the customer, invoking banking protocol, limiting account activity or delaying payment authorisation.</u>	• <u>The firm fails to provide appropriate evidence or audit trails in relation to fraud alert investigations when requested by regulators or law enforcement agencies.</u>
• <u>The firm provides suitable training and support to staff to help identify signs of vulnerability that could potentially increase the risk of fraud occurring.</u>	• <u>Firms are only aware of customer vulnerabilities after the fraud has occurred, limiting the ability to apply preventative measures earlier.</u>
• <u>Customer warnings are deployed at appropriate stages of the payment journey to influence customer behaviour and help prevent APP fraud. The warnings are risk based, understandable, specific to the customer profile, and timely (ie, deployed appropriately along the payment journey, such as when new payees are created, when payees are amended or before payment authorisation).</u>	• <u>Firms do not review or assess the impact customer warnings to determine their effectiveness or determine what changes to the warnings process are needed.</u>
• <u>Where the firm is seeking to use regulation 86(2A) to (2D) of the <i>Payment Services Regulations</i> to delay a payment transaction, the firm uses information gathered through onboarding and ongoing monitoring to help assess whether the threshold for reasonable grounds to suspect fraud or dishonesty has been met.</u>	• <u>The firm allocates an excessive number of accounts, either individual or commercial, for staff members to monitor.</u>

• <u>Firms consider whether enhanced monitoring of, or engagement with, known victims is required to detect unusual activity, or whether certain account restrictions can help reduce the risk of re-victimisation.</u>	• <u>The ongoing monitoring of individual or commercial accounts is allocated to customer-facing staff incentivised to bring in or retain business.</u>
• <u>Cryptoasset businesses pre-screen outbound transactions for addresses linked to fraud.</u>	

<u>Money mules</u>	
<u>Examples of good practice</u>	<u>Examples of poor practice</u>
• <u>The firm considers the holistic information gathered at onboarding to help inform its ongoing monitoring of money mule indicators. This can include assessing whether:</u> ○ <u>account turnover is in line with expectations;</u> ○ <u>more than one customer is using the same device;</u> ○ <u>accounts are accessed in different locations to those identified at onboarding; and</u> ○ <u>virtual addresses are being used and, if so, whether there are valid explanations for such usage.</u>	• <u>The firm focuses on outbound transaction monitoring with no, or limited, consideration of inbound transactions or the holistic information gathered at onboarding.</u>
• <u>The firm undertakes transaction monitoring on inbound and outbound transactions. Monitoring transaction patterns or account behaviours on inbound transactions helps detect unusual activity associated with money mules, such as changes in dormant accounts or rapid turnover in funds.</u>	• <u>The firm does not regularly test and calibrate alert thresholds or is taking too long to implement changes to thresholds, making it slower to respond to emerging threats.</u>
• <u>The firm considers indicators of money mule risk and activity</u>	• <u>The firm does not consider the different ways the proceeds of</u>

<u>beyond the initial receiving account, including linked accounts within the institution, payment characteristics, the broader transaction context and customer behaviour.</u>	<u>fraud may be moved across different fraud types and applies the same approach to monitoring money mule activity across all fraud risks.</u>
• <u>Transaction monitoring rules (dynamic or static) are developed using the customer information obtained at onboarding, are built to detect potential red flags relating to money mule activity, and include appropriate thresholds for creating alerts.</u>	• <u>The firm has inadequate feedback loops in place, meaning alerts are investigated and closed down without an assessment of follow-up action required to update systems and controls, transaction monitoring rules or alert thresholds.</u>
• <u>Alerts arising from transaction monitoring or a money mule account detection tool are investigated promptly by appropriately resourced and trained teams.</u>	• <u>Staff are not adequately trained to understand potential red flags associated with customer behaviour and how these can be associated with money mule activity. As a result, the firm fails to identify and respond swiftly to red flags and fails to prevent funds being moved through mule accounts.</u>
• <u>Where machine learning tools are used to assist with ongoing monitoring, a firm ensures they are used in a way that is proportionate to the size and complexity of its business. Key staff understand how the tools work to ensure transactions are monitored effectively, as well as undertaking regular testing and calibration.</u>	• <u>The firm relies on machine learning tools which are not adequately integrated with the firm's wider systems and controls for identifying and monitoring money mule indicators.</u>
• <u>The firm has policies and procedures in place for setting out its response to suspected and confirmed money mule activity. This can include offboarding, account restrictions and enhanced monitoring (where relationships are retained).</u>	

Reporting

4.2.1L

As set out in *FCG 3.2.10*, firms must have a nominated officer who has a legal obligation to **report any knowledge or suspicions** of money laundering to the NCA through a suspicious activity report (SAR). Where firms know or suspect that fraudulent activity has resulted in money laundering, the nominated officer must report this through a SAR. Firms should also have policies and procedures in place for reporting instances of fraud to the relevant authorities, such as Report Fraud or relevant law enforcement agencies.

Fraud databases play an important role in helping firms detect and prevent fraud. The value firms gain from using these databases, and the value they provide to the cross-system approach to tackling fraud, is contingent on engagement from industry participants in providing reliable and credible intel. Reporting on fraud data at an industry level plays a key role in tackling fraud across the whole system, where sharing a range of information can help firms develop improved mitigation tactics and help identify emerging fraud trends or risks.

We encourage firms, where appropriate and subject to legal and regulatory requirements, to share key fraud information through public-sector or industry-led data sharing initiatives, act on information received and meaningfully contribute to any industry databases they use to support their systems and controls. This is separate from, and does not affect, firms' SAR reporting obligations.

<u>APP fraud</u>	
<u>Examples of good practice</u>	<u>Examples of poor practice</u>
Firms analyse internal fraud data to identify key trends in APP fraud typologies and engage with cross-system initiatives for data sharing to assist other firms with their efforts to detect and prevent fraud.	The firm fails to act appropriately, and in a timely manner, following the receipt of specific intelligence or alert information from industry peers, law enforcement agency or other relevant authority in relation to APP fraud.
Firms which have suspicions about customers or accounts associated with APP fraud share relevant information with other firms promptly and efficiently, to assist efforts to investigate fraud claims.	
The firm takes proactive steps to analyse information received from relevant data sharing initiatives to determine whether similar trends exist in its own	

<u>business. Where relevant trends are identified, the firm takes steps to update staff and help raise customer awareness.</u>	
--	--

<u>Money mules</u>	
<u>Examples of good practice</u>	<u>Examples of poor practice</u>
<u>Firms assess money mule cases individually, and promptly report all relevant cases to the relevant industry-led database.</u>	<u>Firms fail to keep comprehensive records relating to decisions to file, or not file, to the relevant industry led database.</u>
<u>Firms engage with data sharing initiatives designed to help identify money mule activity or networks, rather than relying solely on their internal data.</u>	<u>Firms that use industry-led databases to conduct money mule checks limit the strength of collective intelligence by failing to upload their own confirmed money mule cases in a timely manner.</u>
	<u>The firm fails to act appropriately, and in a timely manner, following the receipt of specific intelligence or alert information from industry peers, law enforcement agencies or other relevant authorities in relation to money mules.</u>

...

Investment fraud

- 4.2.5 ~~UK consumers are targeted by share sale frauds and other scams including land banking frauds, unauthorised collective investment schemes and Ponzi schemes. Customers of UK deposit takers may fall victim to these frauds, or be complicit in them. We expect these risks to be considered as part of deposit takers' risk assessments, and for this to inform management's decisions about the allocation of resources to a) the detection of fraudsters among the customer base and b) the protection of potential victims. [deleted]~~

Self-assessment questions:

- ~~Have the risks of investment fraud (and other frauds where customers and third parties suffer losses) been considered by the firm?~~
- ~~Are resources allocated to mitigating these risks as the result of purposive decisions by management?~~

- Are the firm's anti-money laundering controls able to identify customers who are complicit in investment fraud?

Examples of good practice	Examples of poor practice
• A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud.
• A bank contacts customers if it suspects a payment is being made to an investment fraudster.	• A bank fails to use actionable, credible information it has about known or suspected perpetrators of investment fraud in its financial crime prevention systems.
• A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.	• Ongoing monitoring of commercial accounts is allocated to customer-facing staff incentivised to bring in or retain business.
	• A bank allocates excessive numbers of commercial accounts to a staff member to monitor.

4.3 Further guidance

...

4.3.2 ...

4.3.3 [FG24/6](#) provides guidance for firms using the Payment Services (Amendment) Regulations 2024 to slow down the processing of outbound APP transactions where they have reasonable grounds to suspect fraud or dishonesty.

4.4 Sources of further information

4.4.1 To find out more about what *FCA* is doing about fraud, see:

- Details of the *FCA*'s ~~Information from Lenders scheme:~~
<https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-lenders>
[Information from Lenders scheme](#)
- Details of the *FCA*'s ~~Information from Brokers scheme:~~
<https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-advisers>
[Information from Brokers scheme](#)
- [Details of the *FCA*'s review into the detection and prevention of money mules](#)
- [Details of the *FCA*'s review into anti-fraud controls and complaint handling in firms \(with a focus on APP fraud\)](#)
- [Details of the *FCA*'s review of romance fraud prevention, detection and supporting victims](#)
- [Details of the *FCA*'s review of the use of the National Fraud Database \(NFD\) and money mule account detection tools](#)
- [The *FCA*'s press release on money mules](#)

To find out more about the Failure to Prevent Fraud Offence, see:

- [The Home Office's guidance on the offence of failure to prevent fraud](#)
- [UK Finance guidance on the failure to prevent fraud offence](#)

4.4.2 The list of other bodies engaged in counter-fraud activities is long, but more information is available from:

- ~~Action Fraud~~ [Action Report Fraud](#), which is the UK's national fraud reporting centre: www.actionfraud.police.uk
- ...
- ~~The City of London Police~~ [City of London Police](#), which has 'lead authority' status in the UK for the investigation of economic crime, including fraud <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/Pages/default.aspx>
- [The National Economic Crime Centre \(NECC\) and National Crime Agency \(NCA\) teams work with partners from across public, private and third sectors to pursue serious and organised fraudsters, block fraud from happening and help people avoid and recover from fraud](#)
- ~~The Fraud Advisory Panel~~ [Fraud Advisory Panel](#), which acts as an independent voice and supporter of the counter fraud community: www.fraudadvisorypanel.org/

5 Data security

5.1 Introduction

...

- 5.1.2 Customers routinely entrust firms with important personal data; ~~if this falls into criminal hands, fraudsters can attempt to undertake transactions in the customer's name.~~ Where that data is compromised, criminals may use it to facilitate fraud, including by impersonating customers or undertaking unauthorised transactions. Firms ~~must take special care of their customers'~~ should protect personal data, and comply with the data protection principles set out in Schedule 1 to the obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 1998 2018. ~~The Information Commissioner's Office provides guidance on the Data Protection Act and the responsibilities it imposes on data controllers and processors. See section 4 and schedule 1 Data Protection Act 1998.~~ Firms should have appropriate systems and controls to prevent, detect and respond to data security incidents that may increase the risk of financial crime. Guidance is available from the Information Commissioner's Office (ICO).

5.2 Themes

Governance

- 5.2.1 ...

Self-assessment questions:

- ~~How is responsibility for data security apportioned?~~
- Does the firm's assessment of data security and financial crime risk consider emerging technologies and digital assets, including vulnerabilities associated with digital asset activities, wallets, distributed ledger technology and third-party service providers?
- ~~Has the firm ever lost customer data? If so, what remedial actions did it take? Did it contact customers? Did it review its systems?~~
- What management information (MI), dashboards or reporting does the firm use to identify, monitor and escalate data security incidents, unauthorised access, vulnerabilities, customer data exposures or breaches? Is MI provided in a sufficiently timely manner to support effective decision-making and remediation?
- ~~How does the firm monitor that suppliers of outsourced services treat customer data appropriately?~~
- How does the firm obtain assurance that technology-enabled or automated financial crime controls operate effectively? Are these controls subject to robust internal audit, external audit, independent testing or validation?

...

Examples of good practice	Examples of poor practice
---------------------------	---------------------------

• There is ~~a clear figurehead~~ <u>an individual of sufficient authority championing the issue of data security.</u>	...
...	
• ~~A firm's plans to respond to data loss incidents~~ <u>are clear and include notifying customers affected by data loss and offering advice to those customers about protective measures. A firm's arrangements for responding to data loss or cyber incidents are clear, proportionate, regularly tested and updated following lessons learned. These arrangements include defined roles and escalation routes, timely regulatory notification processes, and a crisis communications plan covering internal communications, customer communications and engagement with relevant third parties, including outsourced service providers, during containment and recovery from a cyber event.</u>	...
...	
• ~~The firm looks at outsourcers' data security practices before doing business, and monitors compliance.~~ <u>The firm assesses an outsourcer's data security arrangements before entering into the relationship and monitors the outsourcer's ongoing compliance with agreed security requirements.</u>	
• <u>The firm regularly reviews data security risks arising from emerging technologies and digital asset-related activities and incorporates these risks into governance reporting, risk</u>	

<u>assessments and control monitoring.</u>	
• <u>Technology-enabled and automated financial crime controls are subject to periodic independent testing and assurance, including review by internal audit and, where appropriate, external specialists.</u>	

Five Six fallacies of data loss and identity fraud

5.2.2

1. **‘The customer data we hold is too limited or too piecemeal to be of value to fraudsters.’** This is misconceived: skilled fraudsters can supplement a small core of data by accessing several different public sources and use impersonation to encourage victims to reveal more. Ultimately, they build up enough information to pose successfully as their victim.
2. **‘Only individuals with a high net worth are attractive targets for identity fraudsters.’** In fact, people of all ages, in all occupations and in all income groups are vulnerable if their data is lost.
3. **‘Only large firms with millions of customers are likely to be targeted.’** Wrong. Even a small firm’s customer database might be sold and re-sold for a substantial sum.
4. **‘The threat to data security is only external.’** This is not always the case. Insiders have more opportunity to steal customer data and may do so either to commit fraud themselves, or to pass it on to organised criminals
5. ~~**‘No customer has ever notified us that their identity has been stolen, so our firm must be impervious to data breaches.’**~~ The truth may be closer to the opposite: firms that successfully detect data loss do so because they have effective risk management systems. Firms with weak controls or monitoring are likely to be oblivious to any loss. Furthermore, when fraud does occur, a victim rarely has the means to identify where their data was lost because data is held in so many places. **‘Partial, historical or seemingly insignificant customer data cannot be valuable to fraudsters.’** Information from multiple sources may be combined to facilitate identity fraud or social engineering attacks. Firms should apply appropriate protections to all customer data, not only complete or current records.
6. **‘Digital identification is foolproof.’** Digital identification and verification tools can improve security but are not immune from abuse. Firms should consider emerging threats such as deepfakes, synthetic identities and AI-enabled spoofing, and regularly review whether their controls remain effective.

Controls

5.2.3

...

Self-assessment questions:

...

- If so, what **levels of security** exist? (For example, does the firm require automatic encryption of laptops that leave the premises, or measures to ensure no sensitive data is taken off-site? If customer data is transferred electronically, does the firm use secure internet links?)
- Where the firm uses AI or machine learning to support fraud detection, customer verification, monitoring or other financial crime controls, how does it ensure that these tools are explainable, appropriately governed and subject to independent validation?
- Does the firm maintain sufficient records, audit trails and decision logs to enable review and investigation of data security incidents, suspicious activity and automated decision-making?
- How does the firm **keep track** of its digital assets?
- How does the firm ensure that customer data is protected when stored, transmitted, backed up or archived? Are encryption standards regularly reviewed and kept up to date?
- How does ~~it~~ the firm **dispose** of documents, computers, and imaging equipment such as photocopiers that retain records of copies? Are accredited suppliers used to, for example, destroy documents and hard disks? How does the firm satisfy itself that data is disposed of competently?
- Does the firm have documented retention, disposal and deletion procedures for customer data, and are these regularly tested to ensure compliance with legal and regulatory requirements?
- How ~~are~~ is **access** to the premises and sensitive areas of the business **controlled**?
- How does the firm obtain assurance that third parties handling customer data maintain appropriate security standards? What arrangements are in place to identify, escalate and respond to third-party data security incidents?

...

Examples of good practice	Examples of poor practice
...	
• The firm understands what checks are done by employment agencies it uses.	...
• <u>Where AI or machine learning tools are used within financial crime controls, the firm</u>	...

<u>understands the operation and limitations of those tools and subjects them to appropriate governance, testing, monitoring and independent validation. The firm can explain and evidence key decisions made by such tools.</u>	
• <u>The firm maintains detailed audit trails, activity logs and records of security-related decisions, and periodically reviews these records to identify control weaknesses, suspicious activity and emerging threats.</u>	...
• <u>Customer data is protected through strong encryption and secure storage arrangements, including for data in transit, data at rest and backup systems.</u>	• Unencrypted electronic data is distributed by post or courier.
• <u>The firm has documented and effective processes for the retention, disposal and deletion of customer data, which comply with applicable legal and regulatory requirements and minimise unnecessary data exposure following the termination of customer relationships.</u>	• <u>The firm deploys automated, AI-enabled or machine learning controls without understanding, oversight, testing or validation of how they operate, including whether they remain effective and resilient to AI-enabled manipulation or other vulnerabilities over time.</u>
• <u>The firm obtains appropriate security assurance from third parties and outsourced service providers that store, process or have access to customer data. Such assurance is subject to ongoing review, independent testing where appropriate, and prompt escalation of material security weaknesses, breaches or control failures.</u>	• <u>The firm cannot demonstrate through audit trails or records how security-related decisions were made or how incidents were investigated.</u>
	• <u>Customer data remains accessible after it is no longer required for business, legal or regulatory purposes.</u>

	The firm relies on contractual assurances from third parties without undertaking ongoing oversight or obtaining evidence that security controls remain effective.
--	---

Effective cyber practices

5.2.3A ...

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 <u>applies patching in a timely manner.</u>	...
The firm ~~carries out regular security testing regularly~~ <u>undertakes penetration testing of its systems and networks and acts promptly to remediate identified vulnerabilities.</u>	Not ~~setting out~~ <u>managing</u> appropriate user privileges on access to resources on the firm's network, data storages or applications.
...	Not encrypting data at storage, eg, 'at rest' or between networks, eg, 'in transit'.
<u>The firm enhances its cyber security arrangements to reflect the growing use of automated systems, including ensuring that automated controls are appropriately governed, monitored and periodically tested to confirm that they remain effective.</u>	...
<u>The firm uses appropriate detection tools to identify threats promptly, contains incidents quickly, maintains secure incident response</u>	...

<u>communications and conducts</u> <u>post-incident reviews to improve</u> <u>future response and recovery</u> <u>arrangements</u>	
...	

...

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

7.1 **Introduction**

7.1.1 **Who should read this chapter?** All firms are required to comply with UK ~~financial~~ sanctions as defined in the Sanctions and Money Laundering Act (SAMLA). Those that are particularly relevant are financial sanctions (including asset freezes) and trade sanctions, hereafter defined as ‘sanctions’. This includes compliance with sanctions relating to counter-terrorist financing and proliferation financing. *FCG 7.2A.14*, which looks at proliferation financing, applies to all firms subject to our supervision.

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*, including authorised cryptoasset businesses and specified investment firms. It also applies to **e-money institutions and, payment institutions and the cryptoasset sector** within our supervisory scope cryptoasset businesses.

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 FCA supervised firms. *FCG 7.2.5G*, which looks at weapons proliferation, applies to all firms subject to our supervision. [deleted]~~

...

7.1.4 ~~Financial sanctions are restrictions put in place by the UK government or the multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds and economic resources in order to achieve a specific foreign policy or national security objective. [deleted]~~

...

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. HM Government publishes the UK Sanctions List, which provides details of those designated under regulations made under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). ~~The list also details which sanctions measures apply to these persons or ships. OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations 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~~ has published guidance on complying with UK obligations and this is available on ~~their website~~ its website. See <https://www.gov.uk/government/publications/financial-sanctions-faqs>.

The Office of Trade Sanctions Implementation (OTSI) within the Department for Business and Trade helps to ensure implementation and enforcement of trade sanctions in the United Kingdom. OTSI provides guidance to assist firms in understanding and complying with trade sanctions regulations. If firms become aware of a breach of UK trade sanctions, they must notify OTSI in accordance with the relevant provisions.

Firms should report to HMRC if the suspected breach relates to breaches of export controls and trade sanctions involving UK customs.

See [government guidance for reporting suspected breaches of trade sanctions](#).

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.~~

- 7.1.6 ~~Alongside financial sanctions, the government imposes controls on certain types of trade. As part of this, the export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Proliferators seek to gain access to this technology illegally: aiding them is an offence under the Anti-Terrorism, Crime and Security Act 2001. Note that the Treasury can also use powers under the Counter Terrorism Act 2008 (see *FCG* Annex 1) to direct financial firms to, say, cease business with certain customers involved in proliferation activity. [deleted]~~

FCG 7.2 is deleted in its entirety. The deleted text is not shown but the section is marked '[deleted]' as indicated below.

7.2 **Themes** [deleted]

Insert the following new section, FCG 7.2A, after FCG 7.2. All the text is new and is not underlined.

[*Editor's note*: although certain provisions in the new section FCG 7.2A have been reproduced from the previous section FCG 7.2, other provisions have been rewritten in their entirety. Accordingly, the section should be read as a whole.]

7.2A **Themes**

- 7.2A.1 The guidance set out in *FCG* 2.2 (Themes) and *FCG* 2.3 (Further guidance) also applies to sanctions.

Governance

7.2A.2 The guidance in *FCG 2.2.1* on governance in relation to financial crime also applies to sanctions.

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 sanctions. Where they identify gaps, they should remediate them.

Self-assessment questions:

- Has the firm **clearly allocated** responsibility for adherence to the sanctions regime? To whom?
- 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 UK sanctions.	• The firm believes payments to sanctioned individuals and entities are permitted when the sums are small. Without a licence from the OFSI, this could be a criminal offence.
• Sanctions compliance is embedded within the wider financial crime control framework. The relevance of wider controls is considered, including adverse media screening, blockchain analysis and transaction monitoring for unusual trading patterns.	• Multinational firms lack the communication between global and regional sanctions teams necessary to manage compliance with UK sanctions laws, regulations and guidance.

There is appropriate escalation of actual target matches and breaches of UK sanctions. Notifications are timely.	No internal audit resource is allocated to monitoring sanctions compliance.
There are controls to ensure administrative, personnel and other payments are not made to designated persons or using sanctioned financial institutions.	Some business units in a large organisation think they are exempt.
The firm conducts horizon scanning and has a plan for instances where overseas operations become subject to sanctions.	The firm fails to investigate and escalate sanctions issues referred to it by external parties.
Staff and senior managers receive sanctions training, which is tailored to the risks facing the business, to ensure that they can discharge their responsibilities effectively.	
The firm has a sanctions policy in place which clearly specifies all sanctions regimes it seeks to comply with, the types of sanctions to which it is exposed and its approach to complying with those sanctions.	

Management information (MI)

7.2A.3 The guidance in *FCG 2.2.2* on MI in relation to financial crime also applies to sanctions.

Senior management should be sufficiently aware of the firm's obligations regarding 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, including changes over time?
- Is the MI produced relevant to UK sanctions?

Examples of good practice	Examples of poor practice
The firm is able to monitor its exposure to sanctions, the efficacy of its sanctions controls, and any crystallised sanctions events.	MI does not explain the nature of any exposure, including whether it relates to financial or trade sanctions issues.
In addition to key metrics around sanctions alerts generated, false positives and true matches, the firm reports further sanctions-related metrics, such as the number of suspected sanctions breaches reported and the time taken for sanctions screening systems to be updated.	
The firm regularly assesses the MI that it collects against new sanctions risk information and guidance, such as OFSI and OTSI publications.	

Risk assessment

7.2A.4 The guidance in *FCG 2.2.4* on risk assessment in relation to financial crime also applies to sanctions and proliferation financing (PF) (see *FCG 7.2A.14* for PF).

A firm should consider which areas of its business:

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

Self-assessment questions:

- Does your firm have a clear understanding of the sanctions risks to the firm and its sanctions exposure? (This may cover different business lines, sales channels, customer types, geographical locations, etc.)
- Does your firm's risk assessment document the sanctions risks faced by the firm, and its assessment of the effectiveness of the control environment?

- Has senior management set a clear risk appetite in relation to its sanctions risks, including in its exposure to sanctioned persons, activities and jurisdictions?
- How is the risk assessment kept up to date, particularly after the firm enters a new jurisdiction or introduces a new product, or where it has identified new sanctions risk events?
- 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?
- Does your firm understand the risk of enablers acting on behalf of a designated person?
- Has your firm assessed its exposure to intermediary countries in sanctions circumvention schemes?
- Has your firm considered its exposure to sanctions measures beyond asset freezes, such as sectoral sanctions or trade sanctions?

Examples of good practice	Examples of poor practice
• A firm with international operations, or that deals in currencies other than sterling, understands the requirements of relevant local financial sanctions regimes.	• There is no process for updating the risk assessment.
• 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 assumes financial sanctions only apply to money transfers and so has not assessed its risks.
• The firm considers sanctions risk across all its business activities and relationships.	• The firm has not documented its assessment of its exposure to financial and trade sanctions.
• A firm performs lessons learned exercises following material sanctions developments to	• The firm assumes trade sanctions only apply to those offering trade finance products.

improve its readiness to respond to future events.	
A 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.	
Where a firm is involved in facilitating international trade, it has mapped its clients' products and associated industries against sanctioned goods and industries.	

Customer due diligence checks

- 7.2A.5 As well as being relevant to other financial crime controls, 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 a firm's CDD process.	A 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 all parties relevant for its screening processes.	The firm's CDD processes are unable to identify connected parties and corporate structures that may be subject to sanctions.
A firm's customer onboarding and due diligence processes are designed to identify customers who make use of corporate vehicles to obscure ownership or source of funds.	A 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.

• A firm has processes designed to identify activity that is not in line with the customer profile or otherwise causes suspicions of sanctions evasion.	• A firm does not capture information relating to potential exposure to trade sanctions as part of its CDD.
• A firm proactively seeks to identify exposure to trade sanctions within its open book and correspondent relationships, in addition to its trade finance operations.	
• A firm takes a risk-based approach to reviewing the sanctions controls and policies of clients and counterparties.	
• A firm uses legal and contractual assurances for compliance (such as sanctions clauses and attestations) in addition to robust customer due diligence processes.	
• Specified sanctions events trigger updates to a firm's CDD/EDD.	
• Where appropriate, a firm takes steps to verify the end-use and end-user in trade transactions to avoid risk of sanctions circumvention, including an assessment of information provided in trade-related documents.	

Further guidance on good and bad practice relating to CDD checks can be found in *FCG* 3.2.4.

Screening customers, counterparties and payments

7.2A.6

Sanctions screening is the process of checking customer, counterparty and transactional data against the relevant sanctions lists to identify potential matches to sanctioned individuals, entities, jurisdictions, goods and services. Compliance with sanctions includes screening names and transactions, applying fuzzy-matching logic to detect variations, and generating alerts of potential sanctions matches for investigation.

Where there are restrictions in relation to specified financial and investment activities, such as in dealing in certain transferable securities or money market instruments, sanctions screening may also involve screening for those activities.

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 to transactions and payments against the UK Sanctions List, and screening existing customers when any amendments are made to the list, helps to ensure that firms will not breach UK sanctions.

Screening policies

7.2A.7

Self-assessment questions:

- If a customer was referred to your firm, how does the firm ensure the person is not designated? (Does the firm screen the customer against the list itself, or does it seek assurances from the referring party?)
- 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? This may also include policies for screening related parties, including directors and ultimate beneficial owners.
- Does your firm have a clear policy on what sanctions regimes it is seeking to screen against, and with what frequency?
- If using an outsourced service, does your firm have appropriate control and oversight of its sanctions screening controls?
- Has your firm documented its consideration of other forms of screening beyond name screening, such as for high-risk jurisdictions or services and goods?

Examples of good practice	Examples of poor practice
• It is clear at what stage customers are screened in different situations (eg, when customers are passed from agents or other companies in the group).	• A firm assumes that an intermediary has screened a customer, but does not check this.
• Where exposure to trade sanctions risk is identified, the firm considers screening for restricted goods and services, high-risk ports and countries, and sanctioned vessels as well as designated persons.	• A firm uses manual screening processes; however, the increasing size of its business has not been considered in its sanctions screening processes.

• A firm screens customers' directors and known beneficial owners on a risk-sensitive basis.	• An insurance company only screens when claims are made on a policy.
• A firm only relies on other firms' screening (such as outsourcers or intermediaries) after taking steps to satisfy itself this is appropriate.	• A firm is overly reliant on a third-party provider screening solution, with no oversight. A firm has no means of monitoring payment instructions.
• 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, including those included on the UK Sanctions List.	• A firm only screens at onboarding and not on an ongoing basis.
• A firm engaging in cryptoasset activities utilises on and off-chain controls to screen customer activities and reacts to possible sanctions evasion, including where exposure or additional information is identified post-transaction, and uses post-transaction controls to inform future risk assessments.	• A firm cannot articulate what is screened for and with what frequency based on its risk assessment.
	• A firm does not assess or document the risk of transactions and aspects of payments messages that are not screened for.

List management and data feeds

7.2A.8

Self-assessment questions:

- When are customers screened against lists, whether the Consolidated List, the UK Sanctions List, internal watchlists maintained by your firm, or lists from commercial providers? (Screening should take place at the time of customer take-on. Good reasons are needed to justify the risk posed by retrospective screening, such as the existence of general licences.)

- What controls does your firm have to become aware of changes or updates to the UK Sanctions List and to then update its systems on a timely basis?
- How does your firm ensure that the updated data is present within the system and that the data quality is complete and accurate within its sanctions screening solution?

Examples of good practice	Examples of poor practice
• A firm has service level agreements regarding list updates through list providers and has processes to ensure the completeness of any updates.	• A firm is unaware of any editorial decisions made by the list provider and therefore is not fully aware what sanctioned entities it is not screening against.

7.2A.9 Calibration, configuration and assurance testing

Self-assessment questions:

- Does your firm evaluate and test its screening capabilities so that its screening system is adequately calibrated to comply with UK sanctions regimes in line with its business requirements?
- Does your firm have a clear governance process for reviewing the calibration of its automated screening systems?
- Has your firm considered how it identifies persons subject to sanctions who are not directly listed on the UK Sanctions List, including where minor variations in naming may exist (for example, entities owned or controlled by designated persons, translated name variations or minor misspellings)?
- Where your firm uses a sanctions screening tool with limited customisation or limited oversight of vendor-implemented settings or processes, has it assessed whether these limitations could impact effective compliance with the UK sanctions regime, and can it demonstrate how those risks are mitigated?

Examples of good practice	Examples of poor practice
• There are quality control checks over manual screening.	• 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.
• A firm understands its automated screening tool and how it is calibrated, and is able to	• A firm has not conducted an adequate assessment of its third-party tools and service

demonstrate that it is appropriate to the firm's risk exposure.	providers to ensure they are capable of supporting compliance with regulatory requirements, nor has it ensured that appropriate governance arrangements and testing have been put in place.
A firm has tested the calibration and configuration of its sanctions screening system and the lists being used and has documented key decisions taken around specific calibration points (for example, the lists used, suppression rules implemented and fuzzy matching threshold).	There is limited or no understanding by the firm about how a third-party tool is calibrated and when lists are updated.
A firm is able to show the controls in place to measure the effectiveness of its automated system, thresholds and parameters – for instance, with sample testing and tuning.	A firm does not review its fuzzy logic calibration.
Where a firm uses automated systems, these can make 'fuzzy matches' (ie, they are 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 potential sanctions breaches.	
A firm escalates any issues identified in its screening system in a timely manner with its screening system provider and is aware of upcoming system updates, changes or fixes.	

Alert management and resourcing

- 7.2A.10 When a customer's name matches a person on the UK Sanctions List, it will often be a 'false positive' (eg, a customer has the same or similar name but is not the same person). Firms should have procedures for identifying where name matches are real and for freezing assets where appropriate.

Self-assessment questions:

- Is the team responsible for sanctions compliance properly resourced and skilled to effectively perform sanctions screening and alert management?
- What steps does your firm take to identify whether a name match is real? (For example, does the firm look at a range of identifier information, such as name, date of birth, address or other customer data?)

Examples of good practice	Examples of poor practice
• A firm's sanctions teams are adequately resourced to avoid backlogs in sanctions screening and are able to react at pace.	• A firm lacks proper resources and expertise to ensure effective screening and investigation of alerts. It has significant backlogs and faces the risk of non-compliance with its obligations.
• Sufficient resources are available to identify 'false positives'.	• Increased volumes and pressure on sanctions teams following changes in the sanctions landscape 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.
• A firm engaging in cryptoasset activities utilises on and off-chain controls to screen customers' activities and reacts to possible sanctions evasion.	• A lack of resources prevents a firm from adequately analysing matches.
• A firm has internal standards at each stage of the process from designation information through to final decision.	• There is no audit trail of decisions where potential target matches are judged to be false positives.

Evasion detection and investigation

- 7.2A.11 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 UK Sanctions List may not always identify potential sanctions evasion involving third parties and alternative detection techniques may be

needed. **Potential red flags for sanctions evasion are set out in alerts issued by the National Economic Crime Centre (NECC).**

OFSI publishes [guidance on threat assessments to support sanctions compliance](#).

OTSI publishes [guidance and blogs to support UK trade sanctions compliance](#).

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

Examples of good practice	Examples of poor practice
• A 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.	• When payments are returned, rejected or queried by correspondent or associated banks, the firm does not seek to understand the cause.
• A firm has proactive, thematic reviews into customers with exposure to high-risk sanction circumvention countries and sectors.	• A firm does not consider the exposure of its customers to high-risk sanction circumvention countries and sectors.
• Following the imposition of significant sanction regime changes, the firm proactively investigates customers with exposure before and after the event in order to detect potential evasion.	
• A firm considers how technology can assist manual interventions to detect sanctions evasion, including vessel tracking and IP tracking.	
• A firm uses tailored transaction monitoring scenarios to detect sanctions evasion.	

• A firm has the technical expertise to identify falsified documentation.	
• A firm has controls and monitoring in place for wire stripping, which might undermine the effectiveness of its screening controls.	

Asset freezing and licences

7.2A.12 When a financial sanction is an asset freeze, the funds and economic resources belonging to or owned, held or controlled by a designated person are generally 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. In addition to asset freezes, OFSI may issue licences for other sanctions measures, including sectoral sanctions and ancillary services bans.

Relevant firms are required to report to OFSI, as soon as practicable, the nature and amount or quantity of any funds or economic resources they hold for a customer who is a designated person.

Additionally, firms are required to report all frozen assets held for designated persons to OFSI annually, including details of all the funds or economic resources frozen in the UK as well as those overseas where the funds or economic resources are subject to UK financial sanctions legislation.

For more information, see OFSI's [guidance on reporting](#).

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 UK sanctions?
- Does your firm have clear policies and procedures to assess, utilise and monitor the use of OFSI licences and statutory exceptions?

Examples of good practice	Examples of poor practice
• A firm proactively engages with clients regarding its use of licences and has controls to ensure compliance.	• Access rights to frozen funds are not controlled. One-off or recurring payments are made from accounts held by designated persons.
• Where the firm maintains an account for a sanctioned individual or entity, the status of	• A firm does not regularly review frozen asset balances or reconcile movements in them.

this account is clearly flagged to staff.	
	An account is not frozen when a match with the UK Sanctions List is identified. If, as a consequence, funds held, owned or controlled by a designated person are dealt with or made available to the designated person, this could be a criminal offence.

Reporting and assessing potential sanctions breaches

7.2A.13 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.

Relevant firms are required to report to OTSI where they know or have reasonable cause to suspect a breach of trade sanctions and should additionally report to HMRC if the suspected breach relates to breaches of export controls and trade sanctions involving UK customs.

In line with *Principle 11*, *SUP 15.3.8G(2)*, *SUP 15.3.11R(1)* 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 its systems and controls.

Additionally, if there are suspicions of money laundering or terrorist financing as a result of sanctions breaches, firms should consider their obligations to submit a Suspicious Activity Report to the UK Financial Intelligence Unit (UKFIU).

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, OTSI 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
A firm undertakes a root cause analysis of potential sanctions	A firm does not report a breach of financial or trade sanctions to

breaches and uses them to update its sanctions controls. The firm's root cause analysis is included in its reporting to OFSI, OTSI and <i>FCA</i> or any other relevant body.	OFSI or OTSI when required to do so . This could be a criminal offence.
After a breach, as well as meeting its formal obligation to notify the relevant authority, the firm reports the breach to the <i>FCA</i>. <i>SUP</i> 15.3 contains general notification requirements. Firms are required to tell us about significant rule breaches (see <i>SUP</i> 15.3.11R(1)), or a significant failure in their financial crime systems and controls.	A firm has poorly defined escalation and reporting procedures to identify to which authority to report.
Significant deficiencies in the firm's systems and controls resulting in potential sanctions breaches are reported to the <i>FCA</i>.	

Proliferation finance

- 7.2A.14 Alongside financial and trade 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*, either as part of the existing practice-wide risk assessment or as a standalone document.

Proliferation financing may utilise mechanisms similar to those used in sanctions evasion, and some proliferation finance measures are implemented through the use of targeted financial sanctions (including asset freezes). As a result, earlier sections of *FCG* 7 on sanctions risks are also relevant, including in relation to customer due diligence, risk assessments, screening, transaction monitoring and evasion detection.

Self-assessment questions:

- Does your firm finance trade with **high-risk countries**? If so, is **enhanced due diligence** carried out on counterparties and goods? Where doubt remains, is evidence sought from exporters that the trade is legitimate?

- Does your firm have **customers from high-risk countries**, or with a history of dealing with individuals and entities from such places? If so, has the firm reviewed how the sanctions situation could affect such counterparties, and discussed with them how they may be affected by relevant regulations?
- What **other business** takes place with high-risk jurisdictions, and what measures are in place to contain the risks of transactions being related to proliferation?
- Does your firm have systems and controls in place to monitor financial services associated with items subject to strategic export controls, including dual use and military goods?
- In addition to sanctions, does your firm conduct appropriate risk assessments in relation to risks of proliferation financing?

Examples of good practice	Examples of poor practice
• A bank has identified whether its customers export goods to high-risk jurisdictions, and subjects transactions to enhanced scrutiny by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern.	• A firm assumes customers selling goods to countries of concern will have checked the exports are legitimate, and does not ask for evidence of this from customers.
• Where doubt exists, the bank asks the customer to demonstrate that appropriate assurances have been gained from relevant government authorities.	• A firm knows that its customers deal with individuals and entities from high-risk jurisdictions but does not communicate with those customers about relevant regulations in place and how they affect them.
• A firm integrates proliferation financing factors into its individual risk assessments, including its country, product, customer and business-wide risk assessments.	• A firm involved with cryptoasset activities lacks adequate transaction monitoring and blockchain analytics capabilities to detect complex transaction patterns, including layering activity or tokens swapped through off-exchange trading via OTC desks or informal brokers, that may indicate proliferation financing risks.
• Following publications of proliferation financing evasion typologies, the firm conducts	• A firm does not conduct a proliferation financing risk

proactive reviews across its portfolio to detect potential exposure.	assessment to consider and document these risks.
	Despite identifying potential exposure to proliferation financing risk, the firm has not adequately incorporated proliferation financing risk factors within its onboarding, customer due diligence, screening and transaction monitoring procedures.
	A firm does not consider the National Risk Assessment of proliferation financing when conducting its own assessment of the risk of proliferation finance.

Case study – deficient sanctions systems and controls

7.2A.15 In October 2024, the *FCA* fined Starling Bank Limited £29m for financial crime failings related to its financial sanctions screening framework.

- In January 2023, Starling identified that, since the implementation of its financial sanctions screening framework in 2017, its automated screening system had only been screening the names of new and existing customers against individuals on the Sanctions List with UK citizenship or UK residency.
- A subsequent review of Starling's financial sanctions framework identified wider systemic weaknesses, including deficiencies in its financial sanctions risk assessment, policies and procedures, the testing and calibration of screening systems, and a lack of effective management information on alert volumes and trends.
- In addition, Starling breached a voluntary requirement (VREQ) restricting it from opening new accounts for high-risk customers, opening over 54,000 accounts for 49,000 high-risk customers between September 2021 and November 2023.

Due to the breaches of the VREQ and *Principle 3* of the *FCA's* Principles for Businesses, the *FCA* imposed a financial penalty of £29m on Starling Bank Limited.

For more information, see the *FCA's* [press release](#).

Case study – OFSI imposition of monetary penalty – Citibank, N.A., London Branch

7.2A.16 In August 2026, OFSI imposed a monetary penalty of approximately £4.7m on Citibank N.A. London Branch for breaches of UK financial sanctions. The

case related to multiple transactions giving rise to breaches across Citibank N.A. London Branch's operations, involving activity across a number of business areas and functions. This included payment processing, correspondent banking and account restrictions.

OFSI's assessment was that many of the breaches arose from specific systems and controls issues and/or errors by Citibank N.A. London Branch staff, or staff in the wider Citi group acting on its behalf. These issues arose in the context of the high volume of Russia-related sanctions designations following the invasion of Ukraine in 2022, which OFSI considered placed significant strain on the bank's alert handling and investigation processes. In particular, delays in the review and escalation of sanctions alerts, and some instances of human error, appear to have contributed to the breaches.

For more information, see OFSI's Public Penalty Notice concerning Citibank, N.A., London Branch.

Amend the following as shown.

7.4 Sources of further information

7.4.1 To find out more on financial sanctions, see:

- ~~OFSI's website: <https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>~~ [OFSI's website](#)
- ~~OFSI provides FAQs on financial sanctions: <https://www.gov.uk/government/publications/financial-sanctions-faqs>~~ [UK financial sanctions guidance](#)
- ~~OFSI's~~ [threat assessments](#)
- ~~Part III of the Joint Money Laundering Steering Group's guidance: www.jmlsg.org.uk~~
- ~~OFSI UK Financial Sanctions Guidance: www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance~~ [OFSI UK Financial Sanctions Guidance](#)
- ~~Alerts~~ [Alerts](#) published by the NECC: ~~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:
 - ~~www.fca.org.uk/russian-invasion-ukraine~~ [Russian invasion of Ukraine](#)
 - ~~www.fca.org.uk/firms/financial-crime/financial-sanctions~~ [Financial sanctions](#)

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

- ~~Part III of the Joint Money Laundering Steering Group's guidance on the prevention of money laundering and terrorist financing, which contains a~~

~~chapter on proliferation financing that should be firms' chief source of guidance on this topic: www.jmlsg.org.uk~~

- The website of the UK's Export Control Organisation [UK's Export Control Organisation](https://www.gov.uk/government/organisations/export-control-organisation), which contains much useful information, including lists of equipment requiring a licence to be exported to any destination, because they are either military items or 'dual use'
~~<https://www.gov.uk/government/organisations/export-control-organisation>~~
- The NCA's website [NCA's website](https://www.nationalcrimeagency.gov.uk/who-we-are/publications/171-sar-guidance-notes/file), which contains guidelines on how to report suspicions related to weapons proliferation: ~~www.nationalcrimeagency.gov.uk/who-we-are/publications/171-sar-guidance-notes/file~~
- The FATF guidance on proliferation financing:
 - ~~www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf~~ [Proliferation financing report](https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf)
 - ~~<http://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html>~~ [Guidance on Proliferation Financing Risk Assessment and Mitigation](https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html)
- HM Government's website, which includes the ~~National Risk Assessment of Proliferation Financing: www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members~~ [National Risk Assessment of Proliferation Financing](https://www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members)
- The Office of Trade Sanctions Implementation (OTSI) helps to ensure that trade sanctions are properly understood, implemented and enforced. OTSI has published guidance regarding trade sanctions, and this is available on its website: ~~www.gov.uk/otsi~~ [website](https://www.gov.uk/otsi)

...

Annex 1 Common terms

Annex 1 ...

[*Editor's note:* Where amendments have been made to the terms in the table below, the terms have moved position in the table to retain the alphabetisation. Those moves are not marked up using strikethrough and underline formatting.]

Term	Meaning
...	
Annex I financial institution	...

<u>APP fraud</u>	<u>Authorised push payment (APP) fraud is where a victim is deceived into authorising a payment either:</u> • <u>to an account that they think belongs to a legitimate payee but is actually controlled by a fraudster; or</u> • <u>for something they believed was legitimate but is actually fraudulent.</u>
...	
<u>CIFAS Cifas</u>	~~CIFAS~~ <u>Cifas</u> is the UK's fraud prevention service with over 250 members across the financial industry and other sectors. See ~~CIFAS's~~ <u>Cifas's website</u> for more information: www.cifas.org.uk.
...	
dual use goods	Items that can have legitimate commercial uses, while also having applications in programmes to develop weapons of mass destruction. Examples may be alloys constructed to tolerances and thresholds sufficiently high for them to be suitable for use in nuclear reactors. Many such goods are listed in ~~EU regulations~~ <u>UK law</u>, which also ~~restrict~~ <u>restricts</u> their unlicensed export.
...	
~~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.~~
...	
fraud (types of)	Fraud can affect firms and their customers in many ways. The following are examples of fraud: ... See also: 'advance fee fraud', '<u>APP fraud</u>', 'boiler room', 'carbon credit scams', 'investment fraud', 'land banking scams', 'long firm fraud', 'mass-marketing fraud', 'Missing Trader Inter-Community fraud', 'Ponzi and pyramid schemes', 'share sale fraud'.
...	
high-value dealer	A firm trading in goods (e.g. cars, jewellery and antiques) that accepts cash of ~~€10,000~~ <u>£10,000</u> or more in payment (whether in one go or in several payments that appear to be linked). HMRC is the supervisory

	authority for high value dealers. A full definition is set out in Regulation 14(1)(a) of the <i>Money Laundering Regulations</i> .
...	
integration	...
~~Production~~ <u>Investigative</u> <u>Court Order</u>	The Proceeds of Crime Act 2002 allows Financial Investigators to use ~~production orders~~ <u>Investigative Court Order</u> to obtain information from financial firms about an individual's financial affairs
...	
Market Abuse Regulation (MAR)	MAR, short for Market Abuse Regulation (EU No.596/2014), entered into force on 3 July 2016 <u>and was onshored into UK law on 31 December 2020 by the EU (Withdrawal) Act 2018</u> . It contains the civil offences of insider dealing, unlawful disclosure of inside information and market manipulation, in addition to provisions to prevent and detect these offences.

[*Editor's note:* the term 'Market Abuse Regulation (MAR)' has been moved to the correct alphabetical position. Amendments to the definition of the term are shown using underlining.]

mass-marketing fraud	~~Action Fraud~~ <u>Report Fraud</u> (the UK's national fraud reporting centre) says "Mass marketing fraud is when you receive an uninvited contact by email, letter, phone or adverts, making false promises to con you out of money." Share sale fraud is a type of mass marketing fraud. See: ~~www.actionfraud.police.uk/types-of-fraud/mass-marketing-fraud~~ <u>Mass marketing fraud</u>
Missing Trader Inter Community (MTIC) fraud	~~This fraud exploits the EU system for rebating Value Added Tax payments in situations where goods have moved across borders within the EU. National authorities are misled into giving rebates to import-export companies that are not entitled to them.~~
...	
Money Laundering Reporting Officer (MLRO)	...
<u>money muling</u>	<u>Money muling is a money laundering technique where criminals use 'money mule' bank accounts to store and transfer criminal funds.</u>
...	
MTIC	~~See 'Missing Trader Inter-Community Fraud'.~~

...	
occasional transaction	Any transaction (carried out other than as part of a business relationship) amounting to ~~€15,000~~ <u>£12,000</u> or more, whether the transaction is carried out in a single operation or several operations which appear to be linked. (See Regulation 27(2) of the <i>Money Laundering Regulations</i>.) Any transaction that amounts to a transfer of funds within the meaning of article 3(9) of the Funds Transfer Regulation exceeding ~~€1,000~~ <u>£800</u>.
...	
reliance	...
~~Action Fraud~~ ~~Report Fraud~~	The UK's national fraud reporting centre. See: ~~www.actionfraud.police.uk~~
...	
sanctions	...
~~Consolidated~~ ~~Sanctions~~ List	~~OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom. It is available from the Treasury's website:~~ ~~www.hmtreasury.gov.uk/fin_sanctions_index.htm~~ 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. The government publishes the UK Sanctions List, which provides details of those designated under regulations made under the Sanctions and Anti-Money Laundering Act 2018.
...	
share sale fraud	Share scams are often run from 'boiler rooms' where fraudsters cold-call investors offering them often worthless, overpriced or even non-existent shares. While they promise high returns, those who invest usually end up losing their money. ~~We have found victims of boiler rooms lose an average of £20,000 to these scams, with as much as £200m lost in the UK each year. Even seasoned investors have been caught out, with the biggest individual loss recorded by the police being £6m. We receive almost 5,000 calls each year from people who think they are victims of boiler room fraud. See:~~ ~~http://seamsmart.fca.org.uk~~ Share, bond and boiler room scams
...	

© Financial Conduct Authority 2026
12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk
All rights reserved

Pub ref: 1-008638

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 0207 066 1000



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