FINANCIAL CRIME GUIDE (AMENDMENT) INSTRUMENT 2024

Powers exercised

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

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

Commencement

B. This instrument comes into force on 29 November 2024.

Amendments to material outside the Handbook

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

Citation

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

By order of the Board
28 November 2024

Annex

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

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

1 Introduction

1.1 What is the FCG?

…

1.1.5 …

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

…

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

Among other requirements, firms should consider whether their financial crime systems and controls are consistent, where applicable, with their Consumer Duty obligations.

For instance, in complying with the Consumer Duty, firms may consider additional steps in their customer journeys to help prevent financial crime, including fraud. They may also consider offering additional consumer support, such as:

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

Firms should consider FG22/5 when applying their financial crime systems and controls. In particular, firms may find it helpful to consider the following provisions:

- *Principle* 12: A firm must act to deliver good outcomes for retail customers;
- Cross-cutting obligations:
  - *PRIN* 2A.2.1R: A firm must act in good faith towards retail customers;
  - *PRIN* 2A.2.8R: A firm must avoid causing foreseeable harm to retail customers; and
  - *PRIN* 2A.2.14R: A firm must enable and support retail customers to pursue their financial objectives; and
- Consumer Duty outcome provisions:
- *PRIN* 2A.5 (Consumer Duty: retail customer outcome on consumer understanding); and
- *PRIN* 2A.6 (Consumer Duty: retail customer outcome on consumer support).

Firms should note that the Consumer Duty does not replace or override other applicable rules, guidance or law and does not require firms to act in a way that is incompatible with any legal or regulatory requirements, such as those under financial crime rules and obligations under the *Money Laundering Regulations*.

1.1.12 To find out more on the Consumer Duty, see 'FG22/5 Final Non-Handbook Guidance for firms on the Consumer Duty' (www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf).

…

3 Money laundering and terrorist financing

…

3.2 Themes

…

The Money Laundering Reporting Officer (MLRO)

3.2.2 …

Firms to which this section applies must appoint an individual as MLRO. The MLRO is responsible for oversight of the firm's compliance with its anti-money laundering obligations and should act as a focal point for the firm's AML activity. Regulation 21(1)(a) of the *Money Laundering Regulations* also requires the appointment of a *senior manager* as the officer responsible for the relevant person's compliance with these regulations. Where appropriate, this section can be relevant to how that person meets their obligations under the *Money Laundering Regulations*. If the MLRO meets the requirements in regulation 21(1)(a) and (3), firms need not make a separate notification to us.

…

Risk assessment

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

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

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

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 to exclude customers inappropriately. Firms must also consider their obligations under the *General data protection regulation*.

Self-assessment questions:

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

Examples of good practice	Examples of poor practice
…	
• The firm has identified good sources of information on money laundering, terrorist financing and PF risks, such as National Risk Assessments, ~~ESA Guidelines,~~	…

FATF mutual evaluations and typology reports, NCA alerts, press reports, court judgements, reports by non-governmental organisations and commercial due diligence providers.	
• Consideration of money laundering, terrorist financing and PF risk associated with individual business relationships takes account of factors such as: o company structures; o political connections; o country risk; o the customer's or beneficial owner's reputation; o source of wealth; o source of funds; o expected account activity; o factors relating to the customer's countries or geographic areas of operations; o products and services; o transactions; o delivery channels; o sector risk; and o involvement in public contracts.	…
• The firm identifies where there is a risk that a relationship manager might become too close to customers to identify and take an objective view of the money laundering risk. It manages that risk effectively.	…
• 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.	

…

Customer due diligence (CDD) checks

3.2.4 …

Self-assessment questions:

…

- Are procedures **sufficiently flexible** to cope with customers who cannot provide more common forms of identification (ID)?
- With **non-face-to-face** transactions, how does 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?

…

Ongoing monitoring

3.2.5 …

Self-assessment questions:

…

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

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

implementing regular periodic reviews and having procedures for event-driven reviews.	
…	

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

The use of transaction monitoring

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

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

This section applies to the use of both automated and manual transaction monitoring, unless specified otherwise.

Self-assessment questions:

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

Examples of good practice	Examples of poor practice
• New approaches are piloted or subject to evaluation periods, with firms able to demonstrate **appropriate testing**.	

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

• A firm **explores** the use of **new approaches** to automated monitoring (e.g. network analysis or machine learning). Consideration is given to the **limitations** of these approaches and how any resultant risks can be contained. (For example, it will not be clear to operators of more free-form varieties of machine learning why the software has made its recommendations, which can pose ethical and audit challenges.)	
• The firm **tailors** the monitoring system rules to its **business, risk and relevant typologies**. The system and rules are **tested and reviewed** for right outcomes	• The firm uses a transaction monitoring system with set rules (which could include use of off-the-shelf systems) and does **not calibrate** these to the **firms' individual needs** or **review** them regularly for efficiency.
• The firm practices **good record keeping**. For example, records of decision making and rationales for thresholds are documented and accessible.	
• Where a firm learns that criminals have abused its facilities, a **review** is performed to **learn** how monitoring methods could be improved to **lessen the risk of recurrence**.	
• The firm using an automated system appropriately **tests and updates parameters** to determine whether a transaction is indicative of potentially suspicious activity.	
	• A firm **does not** check that a **counterparty** firm is monitoring customer activity.
• A firm using an automated system keeps records of how the system has been trained. It records the process for making adjustments and	• A firm using an automated system **lacks an understanding of what the system is detecting and why**. This may be because of, for example, staff turnover, poor

how the interpretable model can be maintained.	documentation or weak communication with the system's vendor.

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

Case study – transaction monitoring

3.2.5B The *FCA* found that 3 key parts of HSBC's transaction monitoring systems showed serious weaknesses over an extended period of several years. The systems were ineffective and not sufficiently risk sensitive for a prolonged period. They exposed the bank and community to avoidable risks.

In particular, the bank failed to:

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

The *FCA* imposed a financial penalty of £63,946,800.

See the *FCA's* press release: www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls.

…

Handling higher risk situations

3.2.7 …

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

- **Correspondent relationships**: where a correspondent credit institution or financial institution, involving the execution of payment, is ~~outside the EEA~~ from a third country (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. JMLSG guidance sets out how firms should apply EDD in differing correspondent trading relationships.

…

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

  (a) a high-risk third country ~~as being one identified by the EU Commission by a delegated act. See EU Regulation 2016/1675 (as amended from time to time)~~ as a country named by FATF on its 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:

  …

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

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

…

…

Customer payments

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

Interbank payments can be abused by criminals. International policymakers have taken steps intended to increase the transparency of interbank payments, allowing law enforcement agencies to more easily trace payments related to, for example, drug trafficking or terrorism. The ~~Funds Transfer Regulation requires~~ *Money Laundering Regulations* require banks to collect and attach information about payers and payees of wire transfers (such as names and addresses~~, or, if a payment moves within the EU, a unique identifier like an account number~~) to payment messages. Banks are also required to check this information is present on inbound payments, and chase missing data. The *FCA* has a legal responsibility to supervise banks' compliance with these requirements. Concerns have also

been raised about interbank transfers known as "cover payments" (see *FCG* Annex 1) that can be abused to disguise funds' origins. To address these concerns, the SWIFT payment messaging system now allows originator and beneficiary information to accompany these payments.

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

…

Case study – poor AML controls

3.2.14 …

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

…

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

3.2.16 …

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

Poor AML controls: risk assessment

3.2.17 …

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

…

3.4 Sources of further information

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

…

- The latest UK National Risk Assessment of money laundering and terrorist financing ~~2017~~ 2020 -

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

www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

…

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

…

- The European Supervisory Authorities (ESAs) have published risk factors guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849- ~~https://www.eba.europa.eu/-/esas-publish-aml-cft-guidelines~~ https://www.eba.europa.eu/sites/default/files/documents/10180/1890686/66ec16d9-0c02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20%28JC%202017%2037%29.pdf

…

3.4.3 To find out more on customer payments, see:

- JMLSG guidance (www.jmlsg.org.uk/guidance/current-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)) ~~of the JMLSG's guidance~~, which will be banks' chief source of guidance on this topic~~: www.jmlsg.org.uk~~.

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

3.4.4 …

3.4.5 To find out more on proliferation financing, see:

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

4 Fraud

…

4.2 Themes

Preventing losses from fraud

4.2.1 …

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

…

Enforcement action against mortgage brokers

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

…

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

…

4.4 Sources of further information

…

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

…

- Fighting Fraud Action (FFA-UK) is responsible for leading the collective fight against financial fraud on behalf of the UK payments industry~~, https://www.financialfraudaction.org.uk/~~.

…

5 Data security

…

5.2 Themes

…

Controls

5.2.3 …

Effective cyber practices

5.2.3A Self-assessment questions:

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

Examples of good practice	Examples of poor practice
	• Using weak or easy to guess passwords or creating passwords from familiar details.

• The firm carries out regular vulnerability assessments and patching.	• Poor physical management and/or control of devices.
• The firm carries out regular security testing.	• Not setting out appropriate user privileges on access to resources on the firm's network, data storages or applications.
• An application programming interface (API) allows different software to communicate with each other and has security measures in place.	• Not encrypting data at storage or between networks.
	• Not updating devices, software and operating systems with the latest security patches.
	• Not properly vetting third-party systems and vendors.
	• Not employing multi-factor authentication for devices, systems and services.
	• Insufficient staff training around social engineering and vishing and phishing campaigns.
• The firm is able to restore systems following an incident and restorations are done in a timely manner.	
	• Inadequate controls to revoke access for staff that leave the firm, the role or the department.

Case study – protecting customers' accounts from criminals

5.2.4 …

For more, see the ~~*FSA's*~~ *FCA's* press release:

~~www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml~~
www.fca.org.uk/news/press-releases/fsa-fines-norwich-union-life-%C2%A3126m-exposing-its-customers-risk-fraud

Case study – data security failings

5.2.5 …

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

~~www.fsa.gov.uk/pages/Library/Communication/PR/2010/134.shtml~~
www.fca.org.uk/news/press-releases/fsa-fines-zurich-insurance-%C2%A32275000-following-loss-46000-policy-holders-personal

…

5.4 Sources of further information

5.4.1 To find out more, see:

- the website of the Information Commissioner's Office: www.ico.org.uk.
- National Cyber Security Centre, 10 Steps to Cyber Security: www.ncsc.gov.uk/collection/10-steps/data-security.
- National Cyber Security Centre, Cyber Security Toolkit for Boards: www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members.

6 Bribery and corruption

…

6.2 Themes

…

Case study – corruption risk

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

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

- ~~Aon Limited failed properly to assess the risks involved in its dealings with overseas third parties and implement effective controls to mitigate those risks.~~
- ~~Its payment procedures did not require adequate levels of due diligence to be carried out.~~
- ~~Its authorisation process did not take into account the higher levels of risk to which certain parts of its business were exposed in the countries in which they operated.~~
- ~~After establishment, neither relationships nor payments were routinely reviewed or monitored.~~

- ~~Aon Limited did not provide relevant staff with sufficient guidance or training on the bribery and corruption risks involved in dealings with overseas third parties.~~
- ~~It failed to ensure that the committees it appointed to oversee these risks received relevant management information or routinely assessed whether bribery and corruption risks were being managed effectively.~~

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

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

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

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

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

See the *FCA's* press release: www.fca.org.uk/news/press-releases/fca-pra-fine-goldman-sachs-international-risk-management-failures-1mdb.

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

6.2.6 …

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

Case study – third parties

6.2.7 In 2022, the *FCA* fined JLT Speciality Limited £7,881,700 for financial crime control failings, which in one instance allowed bribery of over $3m to take place. The firm failed to consider whether additional safeguards or approvals should be incorporated into processes in respect to overseas introducers engaged by another

group entity, where the introduced business was placed by the firm in the London market. Among other issues, the firm's third-party risk assessments failed to:

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

See the *FCA's* press release: www.fca.org.uk/news/press-releases/jlt-specialty-limited-fined-7.8m-pounds-financial-crime-control-failings.

…

6.4 Sources of further information

6.4.1 To find out more, see:

…

- The Ministry of Justice's guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing: ~~https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf~~ https://assets.publishing.service.gov.uk/media/5d80cfc3ed915d51e9aff85a/bribery-act-2010-guidance.pdf (full version) ~~https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-quick-start-guide.pdf~~ https://assets.publishing.service.gov.uk/media/5d80cfd5ed915d5257b5b693/bribery-act-2010-quick-start-guide.pdf (quick start guide)

…

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

7.1 Introduction

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

7.1.2 Firms' systems and controls should also address, where relevant, the risks they face from weapons proliferators, although these risks will be very low for the majority of ~~*FSA* supervised~~ *FCA*-supervised firms. *FCG* 7.2.5G, which looks at

weapons proliferation, applies to ~~**banks carrying out trade finance business** and those engaged in other activities, such as~~ **project finance** and **insurance**~~, for whom the risks are greatest~~ all firms subject to our supervision.

…

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

Under *Principle* 11 (*PRIN* 2.1.1R), we expect authorised firms to notify us if they (or their group companies, *approved persons*, *senior management functions*, *appointed representatives* and *agents*) are targets **of UK** sanctions **or those of any other country or jurisdiction**.

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

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. 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~~, the European Union~~ and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify OFSI in accordance with the relevant provisions. OFSI have published guidance on complying with UK obligations and this is available on their website. See https://www.gov.uk/government/publications/financial-sanctions-faqs.

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

…

7.2 Themes

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

Governance

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

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

Self-assessment questions:

…

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

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

The offence will depend on the sanctions provisions breached.

Management information (MI)

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

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

Self-assessment questions:

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

Risk assessment

7.2.2 The guidance in *FCG* 2.2.4G on risk assessment in relation to financial crime also applies to sanctions and proliferation financing (PF) (see *FCG* 7.2.5G 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 Consolidated List~~.~~;
- are owned and controlled by individuals or entities on the Consolidated List;
- engage in services or transactions prohibited under UK financial sanctions; or
- rely on prohibited suppliers, intermediaries or counterparties.

Self-assessment questions:

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

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

Examples of good practice	Examples of poor practice
…	
• A small firm is **aware** of sanctions regime and where it is most vulnerable, even if risk assessment is only informal.	…
• The firm conducts **contingency planning**, taking a proactive approach to identifying sanctions exposure and is conducting exposure assessments and scenario planning. The firm updates business-wide and customer risk assessments to **account for changes** in the nature and type of sanctions measures.	
• The firm **performs lessons learned** exercises following material sanctions developments to improve its readiness to respond to future events.	
• The firm engages with **public-private partnerships and private-private partnerships** to gather insights on the latest typologies and additional controls that might be relevant and share its own best practice examples.	

Customer due diligence checks

7.2.2A 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 the firm's CDD process.	• The firm has **low-quality** CDD and KYC assessments and **review backlogs**, raising the risk of not identifying sanctioned individuals and entities.
• The firm's CDD identifies **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.
• The 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.	• The firm's CDD **does not articulate** full ownership structures of entities and the firm is unable to show that it is screening all relevant parties.
• The firm **has processes designed** to **identify** activity that is **not in line with the customer profile** or is otherwise **suspicious.**	

7.2.2B Further guidance on good and bad practice relating to CDD checks can be found in *FCG* 3.2.4G.

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

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

Self-assessment questions:

…

- How does the firm become **aware of changes** to the Consolidated List? (Are there manual or automated systems? Are customer lists rescreened after each update is issued?)
- Does your firm have a **clear policy** on which customers, counterparties and payments are subject to screening, and what related data is subject to screening?
- Does your firm have **service level agreements** that cover how quickly it updates its sanctions screening lists following updates to the Consolidated List and that are appropriate to the sanctions risks of its business?

- Does your firm **evaluate** its **screening capabilities** so that its screening system is adequately calibrated for its needs and to monitor UK sanctions? Do you regularly **test/measure** the effectiveness of the system?
- Is the team responsible for sanctions compliance properly **resourced and skilled** to effectively perform sanctions screening **and alert management**?
- If using an outsourced service, does your firm have appropriate **control and oversight** of its sanctions screening controls?

Examples of good practice	Examples of poor practice
…	
• There are quality control checks over **manual screening**.	…
• The firm **understands its automated** screening tool and how it is calibrated, and is able to demonstrate that it is appropriate to the firm's risk exposure.	• Calibration is **not adequately tailored** and the system is either too sensitive or not sensitive enough. This may result in name variations not being detected, for example.
• The firm is able to show the controls in place to **measure the effectiveness** of **its automated** system, thresholds and parameters – for instance, with sample testing and tuning.	• There is **limited or no understanding** by the firm about how a third-party tool is calibrated and when lists are updated.
• Where a firm uses automated systems, these can make '**fuzzy matches**' (e.g. able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.). The firm continually seeks ways to enhance the system to help identify **potential** sanctions **breaches**.	…
…	
• Where the firm maintains an account for a listed individual or entity, the status of this account is **clearly flagged** to staff.	…

• A firm only ~~places faith in~~ relies on **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy ~~themselves~~ itself this is appropriate.	• The firm is **overly reliant** on a third-party provider screening solution, with no oversight. The firm has **no means** of monitoring payment instructions.
• The screening tool is **calibrated and tailored** to the firm's **risk** and **is** appropriate for **screening UK sanctions**. Customers and their transactions are screened against relevant updated sanctions lists and effective re-screening is in place to identify activity that may indicate sanctions breaches.	
• Where **blockchain analytics** solutions are deployed, the firm ensures that compliance teams **understand** how these capabilities can be best used to identify transactions linked to higher risk wallet addresses, **including those included on the Consolidated List**.	
• The firm's sanctions teams are adequately **resourced** to avoid backlogs in sanctions screening and are able to react to those at pace.	• The firm **lacks proper resources** and **expertise** to ensure effective screening **and investigation of alerts**. It has significant backlogs and faces the risk of non-compliance with its obligations.
	• 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.

Evasion detection and investigation

7.2.3A A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. However, simple screening of names against the Consolidated List may not always identify potential sanctions evasion

involving third parties and alternative detection techniques may be needed. **Potential red flags for sanctions evasion are set out in alerts issued by the National Economic Crime Centre (NECC).**

Self-assessment questions:

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

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

Asset freezing and licenses

7.2.3B When a financial sanction is an asset freeze, 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.

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?

Reporting and assessing potential sanctions breaches

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

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

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

Self-assessment questions:

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

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

…

Weapons proliferation

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

…

…

7.3 Further guidance

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

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

  …

7.4 Sources of further information

7.4.1 To find out more on financial sanctions, see:

…

- Part III of the Joint Money Laundering Steering Group's guidance~~, which is a chief source of guidance for firms on this topic~~: www.jmlsg.org.uk
- OFSI UK Financial Sanctions Guidance: www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance
- 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
  - www.fca.org.uk/firms/financial-crime/financial-sanctions

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

…

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

~~http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.~~

- The FATF guidance on proliferation financing:
  - www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf
  - 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
- 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

…

Annex Common terms

Annex 1 Common terms

Annex 1 …

Term	Meaning
…	
Data Protection Act 1998 (DPA)	…
ECCTA	The Economic Crime and Corporate Transparency Act 2023
…	