Consumer credit: Protecting your business from financial crime

November 2016

Financial Conduct Authority

FCA
FINANCIAL CONDUCT AUTHORITY

Contents

Is this booklet for you?

This booklet is for consumer credit firms: in particular, those that are new to being regulated by us. It provides a high-level FCA guide to financial crime. In it, we explain:

- Examples of good and poor practice for businesses under the Money Laundering Regulations 2007 (MLRs), relevant to consumer credit businesses.

- Guidance to firms on steps that can be taken to reduce financial crime risk.

The aim of this guide is to enhance understanding of the FCA's expectations and help you to assess the adequacy of your financial crime system and controls.

Your financial crime obligations

We require all consumer credit firms to put in place systems and controls to mitigate the risk that they may be used to further financial crime. We will look at measures that you take to monitor, detect and prevent financial crime risk. The FCA's financial crime rules are set out in SYSC 6.3.

We are responsible for supervising how some consumer credit firms comply with the MLRs. The MLRs will generally only apply if you are entering into regulated credit agreements as a lender. There are additional anti-money laundering (AML) rules in the Handbook for these firms, set out in SYSC 6.3.6–6.3.10, including the requirements for most consumer credit firms, other than sole practitioners and limited permission firms, to appoint a money laundering reporting officer (MLRO).

If you are only offering fixed sum credit with deferred payments of less than 12 months, then the MLRs will not apply to that part of your business. If you are offering cheque cashing, currency exchange or money transmission (known collectively as Money Service Business), then you will be supervised by HMRC for your compliance with the MLRs. This is the relevant part of the HMRC website for AML supervision of Money Service Business.

1. www.fca.org.uk/static/documents/fsa-journey-to-the-fca.pdf
2. www.fca.org.uk/static/documents/fca-approach-advancing-objectives.pdf

Financial crime systems and controls

Risk assessment

You should identify and assess the financial crime risks to which your business is exposed. This risk assessment should be proportionate to the nature and scale of your firm's activities, taking into account a range of factors, such as the products and services you offer and the way in which your transactions are conducted (e.g. are they non face-to-face?). For further information please refer to the: Joint Money Laundering Steering Group www.jmlsg.org.uk.

Self-assessment questions

- What are the main financial crime risks to your business?
- Does the risk assessment enable you to apply the appropriate level of due diligence to manage the identified risks?
- When did your firm last update its risk assessment?

Examples of good practice

- Your firm assesses where risks are greater and concentrates its resources accordingly.
- Your firm's risk assessment is a continuous process based on a wide range of factors.

Examples of poor practice

- Risk assessment is a one-off exercise.
- Risk assessments are incomplete.

Policies and procedures

We expect your firm to have up-to-date policies and procedures appropriate to its business. These should be readily accessible, effective and understood by all relevant staff.

Self-assessment questions

- How often are your firm's policies and procedures reviewed?
- What steps does your firm take to ensure that staff understand your policies and procedures, and understand how to report suspicious transactions (where relevant)?

Examples of good practice

- There is clear documentation of your firm's approach to complying with its legal and regulatory requirements in relation to financial crime.
- Policies and procedures are regularly reviewed and updated.

Examples of poor practice

- Your firm has no written policies and procedures.
- Your firm fails to check whether policies and procedures are applied consistently and effectively.

Governance

We expect senior management to be actively engaged in your firm's approach to addressing financial crime risk. This includes being aware of the financial crime risks to which your firm is exposed.

Your firm's governance structure should be appropriate to the nature, scale and complexity of your business.

Self-assessment questions

- Who has overall responsibility for establishing and maintaining effective financial crime controls?
- Are they sufficiently senior?
- How are senior management kept up to date on financial crime issues?

Examples of good practice

- Senior management set the right tone and demonstrate leadership on financial crime issues.
- Your firm takes active steps to prevent criminals taking advantage of your services.

Examples of poor practice

- There are no clear allocated responsibilities for financial crime issues.
- There is no meaningful record or evidence of senior management considering financial crime risks.

Staff awareness

Firms must employ staff who possess the knowledge to carry out their functions effectively. To help ensure this, you should provide relevant, financial crime training for staff in key roles.

Self-assessment questions

- How does your firm ensure that its employees are aware of financial crime risks, their obligations in relation to those risks, and how to report suspicious transactions?
- Do your staff have access to training on an appropriate range of financial crime risks?

Examples of good practice

- Ongoing monitoring of employees' work to ensure they understand the financial crime risks relating to your firm.
- Relevant training is in place to ensure staff knowledge is adequate and up to date.

Examples of poor practice

- Staff are not competent to carry out their role effectively, exposing your firm to financial crime risk.
- Relevant staff are unaware of your firm's financial crime issues.
- No financial crime training is given to staff.

Data security

Firms should be alert to the financial crime risks associated with holding customer data and have written data security policies and appropriate systems and controls in place to ensure customer data is kept safe.

Self-assessment questions

- Who has overall responsibility for maintaining effective data security controls?
- Are they sufficiently senior?
- How does the firm monitor that suppliers of outsourced services treat customer data appropriately?

Examples of good practice

- There is clear allocated responsibly for the oversight of data security.
- Your firm has individual user accounts for all systems containing customer data.
- Access to sensitive areas (call centres, server rooms, filing rooms, etc.) is restricted.
- Customer data in electronic form (USB sticks, CDs, hard disks, etc.) is always encrypted.

Examples of poor practice

- Data security is treated as an IT or privacy issue, without recognition of the financial crime risk.
- Staff and third-party suppliers can access data they do not need for their role.
- Password standards are not robust and individuals share passwords.

Anti-money laundering

This guidance is less relevant for those who are not subject to the MLRs, such as debt management firms and credit brokers. It may, however, still be of use, for example, to assist you in establishing and maintaining systems and controls to reduce the risk that the firm may be used to handle the proceeds of crime, and to meet the requirements of the Proceeds of Crime Act 2002 (POCA). An example of this would be making a suspicious activity report. For further information on POCA see www.legislation.gov.uk/ukpga/2002/29/contents.

Customer due diligence (CDD)

Firms must identify their customers and, where applicable, their beneficial owners, and then verify their identities. Firms must also understand the purpose and intended nature of the customer's business relationship.

Self-assessment questions

- Do your CDD processes provide you with a comprehensive understanding of the risk associated with individuals and their business relationships?
- How are issues that are flagged during the due diligence process followed up and resolved?

Examples of good practice

- Your firm understands and documents the ownership and control structures of customers and their beneficial owners.
- Your firm obtains sufficient information about the purpose and nature of the customer relationship and is satisfied that it understands the associated money-laundering risks.

Examples of poor practice

- Procedures are not risk-based: your firm applies the same CDD measures to products and customers of varying risk.
- Your firm has no method for tracking whether checks on customers are complete.

Enhanced due diligence (EDD)

In situations that present a higher risk of money laundering, firms must carry out EDD. EDD should give firms a greater understanding of the customer and their associated risk than standard CDD.

Self-assessment questions

- How does EDD differ from standard CDD?
- How is EDD information gathered and analysed? Is this adequately documented?
- What involvement do senior management or committees have in approving high risk customers?

Examples of good practice

- Your firm proactively follows up gaps in and updates CDD with higher-risk customers.
- Your firm obtains more robust verification of the beneficial owner's identity from a reliable and independent source.
- Your firm establishes the source of the customer's or beneficial owner's funds to be satisified that they do not constitute the proceeds of crime.

Examples of poor practice

- Your firm considers the credit risk posed by the customer but not the money laundering risk.
- Your firm has no procedures for dealing with situations requiring EDD.

Ongoing monitoring and suspicious activity reporting

A firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means scrutinising transactions to ensure that they are consistent with what the firm knows about the customer and may include reviews of customer relationships on a risk sensitive basis.

Self-assessment questions

- Do your staff know to whom they should report suspicious activity?
- How are transactions monitored to spot potential money laundering?
- How are unusual transactions reviewed? How does your firm decide whether behaviour really is suspicious?
- Do you review higher risk relationships regularly to ensure you are comfortable with how they are operating?

Examples of good practice

- Your firm takes advantage of customer contact as an opportunity to update due diligence information.
- Your firm uses monitoring results to review whether CDD remains adequate.
- Higher-risk customers are more closely monitored to confirm expected account activity.

Examples of poor practice

- Your firm fails to take adequate measures to understand the risk associated with the business relationship and is therefore unable to conduct meaningful monitoring.
- Staff always accept a customer's explanation for unusual transactions at face value and do not probe further.
- Suspicious activity is not reported.

Record keeping

Firms must keep evidence of the customer's identity for five years after the business relationship ends. Similarly, transactional documents must also be kept for five years following the completion of the transaction. For further information, please refer to Regulation 20 (4) of the MLRs, which specifically provides that this must form part of a firm's policies and procedures.

Self-assessment questions

- Are customer records readily available to assist ongoing monitoring of customer relationships?

- Can your firm retrieve records promptly in response to a regulatory or law enforcement request?

Examples of good practice

- Records of customer identification and transaction data can be retrieved quickly and without delay.
- Where your firm relies on checks done by a third party, it requests sample documents to test their reliability.

Examples of poor practice

- Your firm keeps customer records and related information in a way that cannot be retrieved in good time.
- Your firm cannot access CDD and related records for which it has relied on a third party. This breaches the MLRs.

Further reading

- Financial crime: a guide for firms Part 1: A Firm's Guide to Preventing Financial Crime
- Financial crime: a guide for firms Part 2: Financial Crime Thematic Reviews
- The JMLSG (Joint Money Laundering Steering Group) Consumer Credit Guidance (should be read in conjunction with JMLSG Guidance Part 1)

More information

- FCA website: Being Regulated: Anti-Money Laundering
- FCA website: Consumer Credit Firms

Financial Conduct Authority

25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk