FINANCIAL CONDUCT AUTHORITY

Money Laundering and Terrorist Financing Risks in the E-Money Sector

Thematic Review
TR18/3

October 2018

Contents

How to navigate this document onscreen

returns you to the contents list

takes you to helpful glossary

1 Introduction

1.1 The aim of the thematic review was to increase our understanding of the risks of money laundering and terrorist financing in the e-money sector. We visited 13 authorised Electronic Money Institutions and registered small Electronic Money Institutions (referred to as 'EMIs') to assess their anti-money laundering (AML) and counter-terrorist financing (CTF) controls. We did not assess other services the EMIs provided, such as money remittance. We also excluded activities outside the FCA's supervisory remit, including gift cards that can be used only within a limited network, or any prepaid product denominated in a cryptocurrency.

1.2 EMIs distribute e-money through a number of channels, including agents and distributors (known as Programme Managers – "PMs"). We were concerned that using PMs may increase money laundering and terrorist financing risks, if firms outsource their commercial activities and due diligence procedures in this way. We therefore also looked at this business model as part of the review.

Executive Summary

1.3 As a result of this diagnostic work, we have a clearer understanding of the potential for harm from money laundering and terrorist financing in the e-money sector. We have also increased our knowledge of e-money firms, and the controls they have in place to mitigate money laundering and terrorist financing risks.

Effective controls

1.4 The majority of EMIs we visited had effective AML systems and controls to mitigate their money laundering and terrorist financing risk. We generally observed a positive culture, and good awareness and understanding of their financial crime obligations. The EMIs generally demonstrated a low financial crime risk appetite. Most have relatively few high-risk customers in their e-money customer base.

Updated policies and procedures

1.5 We found that most EMIs had revised and updated their policies and procedures to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs). This included amending their customer due diligence (CDD) processes to take account of the lower transaction thresholds and other changes to simplified due diligence (SDD) in the MLRs, compared to the 2007 Money Laundering Regulations. Only one EMI had not fully implemented the new requirements but was adopting these at the time of our visit.

1.6 Firms took a number of approaches to comply with changes in the MLRs to due diligence measures and limits, including:

- no longer providing e-money products previously offered under SDD, to either new or existing customers
- requiring existing customers, onboarded under the SDD provisions of the Money Laundering Regulations 2007, to undergo complete CDD

- phasing out prepaid cards issued using the previous SDD provisions - EMIs required existing customers to undergo full CDD if they wished to retain the business relationship

- establishing a 'lifetime' spending limit for e-money products issued under SDD, for existing customers and new customers, after which the EMI will either complete CDD or close the business relationship

Effective monitoring

1.7 At most firms, we found that transaction monitoring was effective and largely based on automated technological solutions.

1.8 The quality of management information in relation to money laundering and terrorist financing varied. Senior management were better engaged and had a more effective understanding where the information had clearly identified key risks supported by data.

1.9 We found that the majority of EMIs with outsourced distribution of e-money and compliance to PMs had adequate governance and audit measures to manage the risks.

Areas not in scope

1.10 Fraud was clearly seen as a key risk by EMIs. This was evident from their business-wide risk assessments, in their transaction monitoring systems and other financial crime controls.

1.11 Another area is the range of other services, as well as e-money products, including money remittance, which may present a higher financial crime risk. The UK National Risk Assessment (NRA) published by the Treasury and the Home Office in 2017[1] assessed the risk associated with money remittance to be high and, therefore, a higher risk business activity than e-money. Firms must therefore ensure their AML and CTF controls are commensurate with the risks posed by this business activity. It should be noted, for completeness, that work on this Thematic review began before the publication of the NRA in October 2017.

1.12 Most firms had a financial crime business-wide risk assessment covering money laundering, terrorist financing (and fraud, as noted). In some firms, this was only in draft, and had not been approved or challenged at Board level. We also found individual customer risk assessments to be less defined in most firms.

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf

2 Overview

Potential money laundering harm from E-Money

2.1 The NRA 2015[2] assessed the money laundering risk of e-money as medium and the terrorist financing risk as low, but this was revised to a medium risk rating by the NRA 2017. The NRA 2015 (section 9.7) recognised that 'open loop[3]' prepaid cards had the potential to be high risk.

2.2 Elements of the products offered by EMIs can increase money laundering and terrorist financing vulnerabilities. These include:

- products that enable cash loading or withdrawals
- an absence of limits on usage, or how much can be loaded on a product
- accounts that permit multiple card users
- situations where no due diligence is required under the MLRs so that consumers can obtain e-money products anonymously
- Use of PMs to distribute products with potential outsourcing risks, such as poor governance and oversight

Financial Crime: Legal requirements on e-money firms

2.3 We undertook our work shortly after the MLRs came into force on 26 June 2017 and tested firms against these obligations. Regulations 37 and 38 of the MLRs introduced some changes which are particularly significant for EMIs:

- Regulation 38 states that issuers of e-money are not required to apply CDD measures if their product meets certain conditions and thresholds. This is provided the EMI monitors its business relationship with users of electronic money and transactions. Thresholds were reduced from those in place under the Money Laundering Regulations 2007
- If a product does not meet the thresholds and other conditions under Regulation 38, an EMI may apply SDD measures in accordance with Regulation 37, where it has assessed the risk to be low

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf

3 An 'open loop' card is an electronic payment card that can be used anywhere the processing brand is accepted (e.g. Visa or MasterCard).

Basis for our findings

2.4 To help us understand this sector, we conducted desk-based analysis of data held by the FCA on e-money firms. This covered their business models, customer numbers and their geographical locations, products offered and transaction values. We visited 13 EMIs between October 2017 and March 2018 to assess their AML, CTF and sanctions systems and controls. We selected a sample representative of the sector, so the firms varied in size, business model, types of products and services offered.

2.5 The assessments comprised:

- a pre-visit review of documents provided by the firms, including financial crime policies and procedures, risk assessments and training materials
- an on-site review, including staff interviews, systems walk-throughs and customer file reviews

Next steps

2.6 We provided individual feedback to all 13 EMIs. We did not find any cases where we needed to use formal supervisory tools to remediate issues.

2.7 We encourage EMIs to review this report, including the examples of good and poor practice, and consider whether their AML and CTF systems and controls could be improved.

3 Findings

Governance, culture and management information

3.1 The senior management of each EMI is responsible for ensuring that the firm's policies, procedures and controls are appropriately designed and implemented. They must also ensure that the firm is operating effectively to reduce the risk of being used for money laundering and terrorist financing.

3.2 This includes having a clear understanding of the money laundering and terrorist financing risks to the firm, and actively ensuring these are managed effectively.

Governance

3.3 We expect EMIs to have a governance structure appropriate to the nature, scale and complexity of their business. Some larger EMIs had management committees where money laundering and terrorist financing risks were regular agenda items. We found that smaller EMIs had a more informal approach to escalating and managing these issues. However, considering the size and scale of these firms, we found this to be equally effective.

Culture and risk appetite

3.4 We found a well-embedded financial crime prevention culture in most of the EMIs. Under the MLRs, EMIs must take appropriate steps to ensure that they identify, assess and mitigate the risks of money laundering and terrorist financing to the business. Overall, we found that EMIs had adequate controls in place to mitigate the risks of money laundering and terrorist financing.

Management Information

3.5 We found that the majority of EMIs produced monthly or quarterly management information reports on fraud, money laundering and terrorist financing. This helped communicate risk exposure to the Board. At smaller EMIs, we found that regular dialogue between senior management and the compliance team enabled them to manage risks effectively. We generally found that senior management at EMIs with clear and effective channels for receiving information, whether formal or informal, were better engaged in AML and CTF issues.

Good practice

Ensuring that key decisions on financial crime issues and follow-up actions are documented, including deadlines and the individual(s) responsible for delivery.

Under Regulation 21(7)(d) of MLRs, EMIs must provide information to senior management at least annually. While an MLRO report is not explicitly required, those EMIs that produced an annual MLRO report found this a useful tool for communicating outcomes and issues.

Poor practice

At one EMI, the outcomes of discussions on money laundering and terrorist financing were not recorded. This included responsibility for actions and deadlines.

Risk Assessment

3.6 Firms must identify and assess money laundering risk. Their risk assessment must be comprehensive and proportionate to the nature, scale and complexity of the firm's business activities. It must be used effectively in setting its risk-based financial crime controls.

Business-wide risk assessment

3.7 The business-wide risk assessment should be constantly reviewed and include any relevant internal and external factors. Most firms had a comprehensive business-wide risk assessment in place. We found risk assessments were better where senior management had assessed and approved them. This involved reasonable challenge to the methodology and content and gave the risk assessment more weight within the business.

3.8 In most cases the risk assessment document included factors such as:

- the use of cash to load products
- potential spending patterns including wallet/card usage in high-risk countries
- identifying higher risk spending
- risks of using PMs to distribute products

3.9 While most firms had a business-wide risk assessment in place, this was not always being used effectively to manage risks. We found some cases where risks had been correctly identified in the business-wide risk assessment, but the appropriate control measures had not been implemented.

Good Practice

Business-wide risk assessments enable high-risk customers to be identified so that enhanced due diligence (EDD) and enhanced ongoing monitoring can be put in place.

Business-wide risk assessments are performed for each product and programme to identify financial crime risks, as well as risk assessing PMs and customers during onboarding.

Poor practice

The business-wide risk assessment is too generic and not tailored to the firm's specific business model and product offerings.

Customer risk assessment

3.10 Individual customer risk assessments are essential to ensure that the risks a customer relationship brings to the firm are captured and that an appropriate risk rating for the customer is established. This helps make due diligence measures and ongoing monitoring effective and proportionate.

3.11 All the firms assessed were screening at onboarding for Politically Exposed Persons (PEPs) and sanctioned individuals. Identified matches were escalated and in the case of PEPs, these were usually approved by the MLRO if the risk fell within the firm's risk appetite.

3.12 Some of the firms assessed had risk tools that would calculate individual customer risk, considering factors such as product type, geographical location, loading and spending volumes. However, these were not always used effectively to trigger EDD and ongoing monitoring.

Good Practice

Having an effective risk scoring method to identify individual customer risk, using factors such as geographical location, expected turnover on account and types of products customers will be using.

Poor practice

Risk scoring methodology developed for corporate customers but not for retail customers. Some retail customers may pose a significant risk even if their transaction volumes and velocities are lower.

One EMI lacked a risk assessment that covered all types of customers at onboarding. The firm therefore had no practical method to establish risk ratings and subsequently apply the appropriate level of CDD to customers.

Policies and procedures

3.13 EMIs must establish and maintain risk-based policies and procedures. This will allow them to mitigate and manage effectively the risks of money laundering and terrorist financing identified in their risk assessments.

3.14 Policies and procedures should be commensurate to the size, complexity and nature of the firm's business. They must take into account new operational, legal and regulatory developments and emerging risks. They must be approved by senior management

and kept under regular review. EMIs must maintain a written record of their policies and procedures, communicate them to all relevant staff and implement them effectively.

3.15 Most of the EMIs visited had adequate AML policies and procedures approved by senior management, which had been updated to reflect legal and regulatory changes.

Good practice

Clearly setting out the behaviours expected of staff and the consequences of not following the firm's AML policies and procedures.

Poor practice

In one firm, the policies and procedures were not clear about when to perform EDD.

Customer Due Diligence

3.16 We found that all EMIs were identifying and verifying customers in line with their obligations under the MLRs. Most customers were onboarded remotely, with identification and verification performed online.

3.17 Where firms did not use online systems, or where electronic verification had been unsuccessful, they employed a manual process to obtain and verify acceptable and valid proof of identity and proof of address from the customer.

3.18 Some EMIs used other electronic tools, such as geolocation software to authenticate the customer's location, as additional CDD measures for non-face-to-face relationships. This also detected cases of multiple (and potentially fraudulent) applications submitted using the same IP address.

3.19 We found firms' CDD was adequate when onboarding corporate customers and PMs. Their processes included identifying and verifying shareholders and beneficial owners of corporate customers and screening them against PEPs and sanctions databases.

3.20 For EMIs operating an outsourcing business model with PMs, CDD was mostly performed by the PM, with oversight from the EMI through measures such as spot-checking and periodic audits. However, in 2 firms, the EMI carried out some of the CDD and the PM performed the rest.

3.21 Where e-money products had a prescribed or restricted use, such as payroll or payment of work-related expenses, the intended purpose of the customer relationship was understood, so no further assessment or information gathering was performed.

3.22 Most EMIs were screening customers for PEP and sanctions at onboarding although the frequency of re-screening varied. Firms are required to take a risk-based approach to ongoing monitoring, including re-screening for PEPs and sanctions.

Good Practice

One EMI used on-site visits as part of their onboarding of PMs to achieve an increased understanding of the PM's systems and controls.

Spot-checking the quality of CDD carried out by PMs, by having access to the PMs' records and systems, to ensure they are complying with the EMI's policies and procedures.

Poor practice

Failing to assess the nature and intended purpose of the relationship. This is an important part of the due diligence process which is essential for effective monitoring of the relationship.

Enhanced Due Diligence

3.23 EDD is required in certain higher risk situations, as well as where firms assess there is an increased risk of money laundering or terrorist financing associated with their customers. The extent and quality of EDD measures must be commensurate with the risks identified. The objective is to increase the firm's understanding of the risks associated with such customers, so they can mitigate these risks effectively. Firms must also monitor higher risk business relationships.

3.24 The MLRs amend the previous definition and scope of a PEP to include those holding relevant positions in the UK and the obligation for firms to perform risk-based EDD for these customers. The FCA has issued guidance on how to apply appropriate EDD measures for different PEPs.[4] The guidance states that UK PEPs should be managed as lower risk, with less intrusive levels of EDD unless other risks of money laundering and terrorist financing exist.

3.25 We found fewer than half of EMIs had onboarded PEPs, with very low numbers of PEP customers generally when compared to total customer numbers. For most retail customers, we found EDD was triggered only if spending thresholds were exceeded.

3.26 Some firms carried out EDD before establishing the business relationship. Examples include where the product was higher risk, such as cross-border use or cards loaded using cash.

3.27 EMIs generally conducted EDD when onboarding business customers. This included sole traders, as their commercial activities involved significantly higher volumes and values, with an increased risk. EDD included on-site visits to their customers and monitoring

4 www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

their websites using specialist providers. For EMIs that used PMs, EDD included interviewing staff at the PM and assessing the PM's financial crime control framework.

3.28 EMIs with higher risk customers, including PEPs, were generally carrying out enhanced ongoing monitoring of these relationships, taking a risk-based approach.

Good Practice

An EMI with concerns about a customer contacted a merchant directly to obtain a more detailed understanding of the customer's business, including source of wealth and source of funds.

Poor practice

At one firm, we saw unclear EDD processes and inadequate guidance to staff, including a lack of detail on the types of information acceptable as evidence of source of wealth and source of funds.

Ongoing monitoring

3.29 Ongoing monitoring is necessary to help identify unusual activity and transactions. If customers cannot provide a reasonable explanation for unusual activities or transactions, these may give rise to suspicions of money laundering or terrorist financing (or fraud). EMIs should consider whether the information they have amounts to reason to suspect money laundering or terrorist financing. If so, this must be reported to the National Crime Agency (NCA). Where a Suspicious Activity Report is submitted, the firm should review whether they should continue the business relationship.

3.30 Regular monitoring of customer activity and transactions throughout the life of a business relationship will help EMIs to know their customers. This will allow them to assess risk, and give them greater assurance that they are not being used for the purposes of financial crime.

Transaction monitoring

3.31 Transaction monitoring does not necessarily require sophisticated electronic systems. It can range from fully manual analysis of transactions to a risk-based review of system-generated alerts. It can also include staff awareness of potentially suspicious activities. We found that automated systems added value for EMIs because they could deal effectively with larger volumes of transactions.

3.32 In larger EMIs, the most effective transaction monitoring system was a 'real-time', rules-based application which generated alerts when unusual activity was detected. In most cases, EMIs followed up alerts with a post-event transaction review, taking appropriate steps to block the account and notify the NCA, where appropriate.

3.33 Most EMIs had set adequate rules in their transaction monitoring systems to identify suspicious transactions. These parameters need to be kept under review, to ensure

they continue to identify suspicions of money laundering and terrorist financing as criminal techniques and money laundering risk evolves.

Periodic reviews

3.34 In most cases, customers were assessed as high, medium or low risk, with EMIs focusing their resources on higher risk relationships, including PEPs. Most EMIs carried out periodic reviews of high-risk relationships. EMIs mainly operated an event-driven review model for low and medium risk relationships. One EMI did not carry out any periodic reviews of its customer base, but had plans to introduce them.

Good practice

Spot-checks are performed on accounts where potentially suspicious activity has been identified to ensure decisions are appropriate and documented.

Daily and weekly transaction monitoring reports including information on loads, spending, jurisdiction and loading method were compiled at one large EMI. These reports were reviewed by the Compliance team.

The principal firm performs its own transaction monitoring of their PMs' underlying customers to ensure compliance with regulation 38(3) of MLRs.

Poor practice

An EMI was not assessing the purpose and intended nature of the business relationship or transaction. This inhibited its ability to perform effective ongoing monitoring and identify suspicious transactions.

Outsourcing

3.35 During the review, we assessed 5 firms with an outsourcing model, using PMs to market and distribute e-money. Often, CDD was conducted by the PM on behalf of the principal firm. Where reliance for CDD is placed on a PM, legal responsibility always remains with the EMI.

3.36 We observed two different models adopted by EMIs for complying with the MLRs when using PMs:

- full outsourcing of AML controls by the principal firm, including customer onboarding, PEP and sanctions screening, risk assessment and monitoring
- hybrid model, where some functions are outsourced to the PM for customer onboarding and PEP and sanctions screening, but other functions are performed by the EMI

3.37 Outsourcing to PMs worked well where governance and oversight was robust and the EMI performed effective audits of the PMs. Effective oversight included dip-sampling files to establish that CDD processes, including sanctions and PEP screening, were performed correctly.

3.38 On-site visits and audits of PMs were also undertaken by firms using a risk-based approach. The factors used by firms to determine which PMs to visit included customer numbers, methods of loading (e.g. cash), types of card wallet spending and geographical location.

3.39 Governance and oversight were also effective where audit plans were used, including dedicated resources allocated within audit or compliance teams. This ensured systematic oversight and follow-up of any weaknesses identified during audits.

3.40 In a few firms, the principal did not conduct regular on-site visits and relied on the PM to operate effectively. However, they did test the PM's systems and controls by conducting file reviews, or requesting management information to confirm that PEP and sanctions screening processes were being carried out effectively.

Good Practice

In one EMI, transaction monitoring had been outsourced to a third-party provider. The EMI received adequate management information and conducted regular on-site visits to ensure outsourced processes were being conducted effectively.

Having an annual audit plan for PMs, taking a risk-based approach and not applying a 'one size fits all' model, to ensure appropriate ongoing monitoring and oversight.

Poor practice

One EMI used very limited resources to conduct and manage assurance assessments of PMs.

Interaction between the EMI and the PM does not include discussions on financial crime matters.

Training, Communication and Awareness

3.41 Firms must ensure that they employ staff with the appropriate skills, knowledge and expertise to perform their functions and responsibilities effectively. Firms must ensure that employees are given training, which must be effective and fit for purpose.

3.42 We found that all 13 EMIs had mandatory annual AML and sanctions training for existing staff members. New joiners are required to complete AML training as part

of their induction process. Two of the EMIs with PMs had provided training to them, covering AML and fraud trends and typologies, as well as sharing best practice.

3.43 We saw differences in delivery channels, with at least half of EMIs providing training through computer-based programmes. About a quarter of EMIs provided staff with both face-to-face and computer-based training. Two firms preferred classroom-based tuition to e-learning. Training was mostly delivered using in-house programmes, although a few EMIs employed external e-learning providers and consultants, particularly for face-to-face tuition.

3.44 A common feature was the requirement for staff to pass an assessment at the end of training. For all EMIs, training was tracked and monitored, with statistics reported as part of the firm's management information.

3.45 We saw some differences in training content. All firms covered money laundering and terrorist financing. Most also included the changes introduced by the MLRs, explaining their impact and significance for the firm. In one EMI, the training content was too basic and focused only on reporting suspicious transactions.

3.46 Attitudes towards external training differed. Staff from over half the EMIs had received external financial crime training, with diverse levels of professional qualifications achieved.

Good practice

Face-to-face training at one EMI consisted of 2 sessions a year and a final assessment. It included case studies which complemented online training material.

Ensuring staff attend industry events on AML and share relevant information with other members of staff.

At one EMI, onboarding teams based overseas were not given access to systems until they had passed basic training. Further training was subsequently provided on a regular basis through quarterly on-site visits by the Compliance team.

Poor practice

Financial crime training was based solely on reporting suspicious activities. Narrow training content may result in staff not being trained effectively on how to apply the firm's AML policies and procedures.

Annex 1
Glossary

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CTF	Counter-Terrorist Financing
EDD	Enhanced Due Diligence
EMI	Electronic Money Institution
FCA	Financial Conduct Authority
JMLSG	Joint Money Laundering Steering Group
MI	Management Information
MLRO	Money Laundering Reporting Officer
MLRs	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
NCA	National Crime Agency
NRA	National Risk Assessment
PEP	Politically Exposed Person
PM	Programme Manager
SDD	Simplified Due Diligence

Pub ref: 005702

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