WILLIAM FRY

// FINANCIAL REGULATION

Central Bank Dear CEO Letter to Payment Institutions and Electronic Money Institutions

January 2023

On 20 January 2023, the Central Bank of Ireland (**Central Bank**) published a Dear CEO Letter to payment institutions (PIs) and electronic money institutions (**EMIs**) outlining recent supervisory findings and reaffirming supervisory expectations for this sector.

The Dear CEO Letter highlights weaknesses and risks within PIs and EMIs. It sets out expectations and actions identified by the Central Bank to remedy deficiencies in five key areas, namely, (i) safeguarding, (ii) governance, risk management, conduct and culture, (iii) business model, strategy and financial resilience, (iv) operational resilience and (v) anti-money laundering and countering terrorist financing. The Dear CEO Letter should promptly be bought to the attention of and considered by the boards of all PIs and EMIs bearing in mind the **31 July 2023** deadline for an audit review and board response regarding compliance with safeguarding requirements.

BACKGROUND

The Dear CEO Letter follows the December 2021 Dear CEO Letter from the Central Bank to PIs and EMIs on its supervisory expectations. It also refers to the recent reference in the International Monetary Fund's (**IMF**) Technical Note on Oversight of Fintech in Ireland of the payment and e-money sector's growing importance within the broader fintech sector in Ireland.

Please see our briefing here for further information on the 2021 Central Bank Dear CEO letter. For a copy of the 2023 Central Bank Dear CEO Letter please see here. Please see here for a copy of the IMF Technical Note on Oversight of Fintech in Ireland.

PRIORITY AREAS FOR THE CENTRAL BANK

The Letter highlights five key areas for attention.

(i) Safeguarding

What is expected

PIs and EMIs must have robust safeguarding arrangements in place to demonstrate that users' funds are properly managed and protected in line with supervisory expectations and obligations under the European Union (Payment Services) Regulations 2018 (as amended) (**PSR**) and European Union (Electronic Money) Regulations 2011 (as amended) **(EMR**). This is demonstrated by firms putting in place risk management frameworks to ensure that users' funds are appropriately identified, managed and protected on an ongoing basis. Safeguarding risk frameworks should include measures providing clear segregation, designation and reconciliation of client balances. The firm's board and each line of defence have an important role to play in the oversight and assurance of safeguarding arrangements.

Weaknesses highlighted

The Central Bank identified the following issues:

- SEGREGATION: delays in segregating users' funds following receipt and co-mingling of users' and non-users' funds in safeguarding accounts.
- DESIGNATION: co-mingling of users' funds and non-user's funds in safeguarding accounts and incorrect designation of bank accounts where users' funds are held.
- RECONCILIATION: failure to reconcile that the correct amounts are being segregated daily.
- INSURANCE POLICIES OR COMPARABLE GUARANTEES: (where relevant) not being maintained on an ongoing basis.
- CONTROL: control over the safeguarding account not resting within the firm (for example, resting with a group entity).
- OVERSIGHT: Insufficient oversight of arrangements for safeguarding users' funds and a lack of policy documentation and effective and regular monitoring and review of safeguarding.
- FEES AND CHARGES: consumer fees/other charges being taken out of the safeguarding account inappropriately.
- OPERATIONAL CHANGES: consideration of operational change impact (including material changes to business strategy) on safeguarding arrangements not being evidenced adequately.

Actions to be taken

Firms must:

- TEST: proactively test safeguarding frameworks on an ongoing basis to ensure they are well-designed and operating effectively.
- NOTIFY: notify the Central Bank immediately of any safeguarding issues identified.
- MITIGATE AND CORRECT: mitigate and correct issues identified to ensure that users' funds are safeguarded.
- INVESTIGATE AND REMEDIATE: investigate the root cause of any safeguarding issue and remediate any problem identified.
- AUDIT: an audit of compliance with the safeguarding requirements under the PSR/EMR (as appropriate) should be carried out by an audit firm. The audit opinion must capture whether the firm maintains adequate organisational arrangements to meet safeguarding requirements under PSR/EMR on an ongoing basis. The audit must cover specific areas of review and assurance (as set out below).
- BOARD RESPONSE: The audit opinion, along with a Board response on the outcome of the audit, should be submitted to the Central Bank by 31 July 2023.

AUDIT REVIEW - SPECIFIC SAFEGUARDING AREAS THAT SHOULD BE SUBJECT TO AUDIT REVIEW:

1. Governance and oversight of safeguarding arrangements (including the roles of the first, second and third lines of defence and the board), taking into consideration the nature, scale and complexity of the firm's business.
2. Safeguarding users' funds under the applicable timeframes required under the PSR/EMR. Testing of the process should be included.
3. Confirmation that safeguarding account(s) are appropriately designated (if segregation method of safeguarding is used).
4. Frequency and accuracy of the administration and reconciliation process to ensure sufficient users' funds are in the firm's designated safeguarding account or that the insurance policy/comparable guarantee is sufficient to meet the firm's safeguarding obligations at all times. Testing of the reconciliation process should be included.
5. Where safeguarded funds are invested in secure, liquid and low risk assets or secure and low risk assets, an Investment policy assessment should be carried out to ensure the assets chosen are liquid, secure and low risk (as appropriate) and that the firm is in a position to manage any associated market risk.
6. Safeguarding account control assessment (to include the number of persons with access to the safeguarding account and their functions). Testing of the controls should be included.
7. Insurance policy/comparable guarantee administration process assessment – including how the firm satisfies itself as to the appropriateness of the policy/guarantee, the process for renewing the policy/guarantee and the process for increasing the level of cover where required or making a claim on the policy/guarantee.
8. Safeguarding breach and incident identification, escalation and management process assessment, including for reporting to the board/Central Bank.
9. Liquidity assessment to ensure that the firm's safeguarding arrangements facilitate the redemption of electronic money at any time and at par value or the timely execution of payment transaction requests (as applicable).

(ii) Governance, risk management, conduct and culture

What is expected

The Central Bank expects firms to embed a consumer-focused culture as evidenced by adequate governance, risk management and internal control frameworks.

Weaknesses highlighted

- MISALIGNMENT BETWEEN BUSINESS GROWTH AND GOVERNANCE, RISK AND CONTROL FRAMEWORKS: Where business growth outpaces the governance, risk management and internal control environment and frameworks of that business this results in governance, risk management and internal control frameworks not being aligned consistently with business strategies and business objectives.
- SUCCESSION PLANNING: Inadequate succession planning (e.g. key positions remaining vacant for a considerable period).
- RESOURCING: Inadequate resourcing (e.g. in internal audit, risk management and compliance functions) resulting in poor governance of compliance activities and assurance work.
- COMPLIANCE FOCUS: Compliance focus being misdirected (e.g. where compliance is viewed as a cost, rather than a business strategy).
- BOARD REPORTING: Customer complaints, fraud levels etc. not being adequately reported to the board.
- DISCLOSURES: Unclear product/service information (e.g. inadequate information on group affiliates, agents or distributors and any related regulatory protections).

Actions to be taken

Boards should consider their governance, risk management and internal control frameworks in addition to the composition (both number and skills) of their board and management teams to ensure they are sufficient to run their business from Ireland as their licenced jurisdiction.

(iii) Business model, strategy and financial resilience

What is expected

PIs and EMIs are expected to have capital-accretive business models and strategies that are viable and sustainable. Firms must have sufficient financial resources to support current and projected business plans (considering firm-specific and market-wide stress scenarios). Firms must also understand and meet own funds requirements on a stand-alone basis and ensure sufficient regulatory capital is available to absorb losses, including in a resolution scenario.

Weaknesses highlighted

- BUSINESS STRATEGY: Lack of defined or embedded board-approved business strategies.
- CAPACITY: Insufficient financial (capital and liquidity) and operational (resources, IT systems etc.) capacity and capability within the firm to execute strategy.
- FINANCIAL PLANNING: Insufficient detail in financial projections and underlying assumptions, including stress scenarios, to underpin their credibility.
- CAPITAL: Failure to ensure sufficient regulatory capital is available to absorb losses, including during stress conditions.
- INACCURATE RETURNS: One in every five firms submitted inaccurate regulatory returns to the Central Bank in the previous 12 months (e.g. incorrect methodologies for calculating own funds, incorrect classification of regulatory capital held, incorrect payment values).
- RESOLUTION PLANNING: Failure to have an appropriate exit/wind-up strategy linked to the firm's business model, which includes provisions on the timely and efficient return of users' funds in a resolution scenario.

Actions to be taken

Firms should have Board approved business strategies in place supported by robust financial projections. Firms must understand and meet their capital requirements at all times. Strong internal controls must be in place that are subject to regular testing to ensure accuracy of data used for regulatory reporting and for strategic and financial planning.

(iv) Operational resilience and outsourcing

What is expected

The Central Bank expects all firms in the financial sector to demonstrate readiness for and resilience to operational disruptions, including, in respect of PIs and EMIs, in particular, a required emphasis on IT risk management.

The three pillars underpinning the Central Bank Cross Industry Guidance on Operational Resilience and Cross Industry Guidance on Outsourcing issued in December 2021, which apply to the financial services sector, including PIs and EMIs, are (i) identify and prepare for, (ii) respond and adapt to and (iii) recover and learn from, an operational disruption.

Please see our Operational Resilience Guidelines and Outsourcing Guidelines briefings for further information.

The Central Bank expects boards and senior management teams of PIs and EMIs to:

i. have the skills and knowledge to meaningfully understand the risks their firm faces and the responsibilities they have (including about outsourced activities where the activities are conducted on the firm's behalf by a third party or group entity); and

ii. review and adopt appropriate measures to strengthen and improve their operational resilience frameworks in line with the above guidelines.

The Central Bank will continue to challenge how firms ensure that risk and control frameworks operate effectively and are prepared for unforeseen operational disruptions.

Weaknesses

- MAJOR IT OUTAGES: The Central Bank has noticed increased major incidents/outages reported by PIs and EMIs. Many arise from issues with group/third-party providers who are critical to supporting the IT infrastructure of firms.

Actions to be taken

CRITICAL OR IMPORTANT SERVICES: PIs and EMIs must view their business operations through the business service lens. Firms must prioritize what is critical or important to their business or the financial system to understand the interconnections and interdependencies involved in delivering those services and determine the impact of a disruption on services.

REVIEW: Review and adopt measures necessary to ensure robust and effective operational resilience frameworks.

(v) Anti-money laundering and countering the financing of terrorism

What is expected

PIs and EMIs are designated persons under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (**CJA 2010**) and are subject to its obligations.

Part 4 of the CJA 2010 obliges firms to implement an effective risk-based anti-money laundering and countering the financing of terrorism (**AML/CFT**) framework, which includes the application of a risk-based approach to ensure that controls put in place are sufficient to mitigate the Money Laundering (**ML**)/Terrorist Financing (**TF**) risks identified. These frameworks should be based on a firm-specific risk assessment, focussing on the particular AML/CFT risks arising from the firm's business model.

As well as complying with legislative and regulatory obligations, firms must comply with their conditions of authorisation issued by the Central Bank and be aware of guidelines and risk factors to consider when assessing ML/TF risk (such as those set out in European Banking Association Guidelines (EBA/GL/2021/02)).

Where customer risk assessments and customer due diligence (**CDD**) on the end user of the products and services are performed by agents and distributors on behalf of firms, the responsibility ultimately rests with firms.

Weaknesses

RISK-BASED APPROACH: (i) lack of a mature risk-based approach, (ii) deficiencies in understanding ML/TF risk meaning that controls are not as robust or extensive as they should be, (iii) transaction monitoring controls not being correctly configured which, in the context of suspicious activity/transactions, can lead to failures in detecting suspicious activity/transactions or excessive alerts impacting reporting timeliness.

DISTRIBUTION CHANNELS: Failure to regard distributors and agents as an extension of the firm and inappropriate oversight of CDD and other AML/CFT preventive measures carried out by agents or distributors on behalf of firms. For example, AML/CFT preventive measures need to be completed in line with the firms' ML/TF risk assessment and AML/CFT policies and procedures.

ELECTRONIC MONEY DEROGATION AND SIMPLIFIED DUE DILIGENCE (SDD): Misapplication of the CDD derogation for certain e-money products under Section 33A of the CJA 2010 and misinterpretation of SDD under Section 34A of the CJA 2010, leading to an incorrect level of CDD being applied to customers in those circumstances.

Actions to be taken

RISK-BASED APPROACH: Firms should better understand how their products and services could be used for ML/TF purposes. AML/CFT controls should be risk-sensitive and tailored to the risks identified as part of the firm's ML/TF risk assessment. Firms should correctly configure transaction monitoring controls to detect where the ML/TF risks identified as part of the firm's ML/TF risk assessment are materialising.

DISTRIBUTION CHANNELS: Firms must exercise adequate oversight (including appropriate assessment) of the agents and distributors with a proper level of ongoing assurance conducted. The outcome of any testing carried out as part of the oversight of these arrangements should be included in management information prepared for the board and senior management.

ELECTRONIC MONEY DEROGATION AND SDD: EMIs should only avail of the derogation contained in Section 33A of the CJA 2010 in circumstances where it is appropriate to do so and where all the criteria have been met. The derogation is not available where other high-risk factors are present, for example, where the customer is a politically exposed person (**PEP**) or where the customer concerned is established or resident in a high-risk third country. SDD must only be carried out where appropriate and where the firm has conducted a risk assessment of each relationship. SDD must be justified based on the lower level of risk presented.

NEXT STEPS FOR CEOS AND BOARDS OR PIS AND EMIS

The Central Bank expects firms to take proactive measures to ensure robust and appropriate governance and control arrangements.

The Central Bank expects the boards of PIs and EMIs to discuss the Dear CEO Letter and to reflect on the supervisory findings called out.

EMIs and PIs must complete a specific audit of compliance with the safeguarding requirements under the PSR/EMR, and submit the audit report, together with the board response, to the Central Bank by 31 July 2023.

William Fry is available to assist PIs and EMIs with their review and assessment of compliance of the firm with the Central Bank's supervisory expectations as set out in the Dear CEO Letter.

CONTACT US

For more information, please contact Shane Kelleher, Louise McNabola or your usual William Fry contact.

Shane Kelleher
PARTNER
Head of Financial Regulation
+353 1 639 5148
shane.kelleher@williamfry.com

Louise McNabola
PARTNER
Banking & Finance
+353 1 639 5196
louise.mcnabola@williamfry.com