Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

T +353 (0)1 224 6000

Bosca PO 559
Baile Átha Cliath 1

PO Box 559
Dublin 1

www.centralbank.ie

20 January 2023

**Re: Supervisory Findings and Expectations for Payment and Electronic Money (E-Money) Firms**

Dear CEO

In September 2021, and effective from January 2022, the Central Bank of Ireland (the Central Bank) published its multi-year Strategy. The Strategy centres around four strategic themes - safeguarding, being future-focused, open and engaged, and transforming. These themes are our way of describing what is important for us as an organisation so that we can meet the challenges of a changing world, and deliver on our mission and vision.

The delivery of our statutory responsibility for regulation and supervision, and our Strategy, will continue to drive our approach to the authorisation and supervision of firms operating in the Payment and E-Money sector, which is an important and growing part of our mandate. In that regard, the recent International Monetary Fund (IMF) Ireland Financial Sector Assessment Program-Technical Note on Oversight of Fintech (the FSAP) noted the increasing importance of the Payment and E-Money sector, which represents one of the largest sub-sectors within the broader fintech universe in Ireland[1].

Our December 2021 Dear CEO letter sought to provide greater clarity on our supervisory expectations for the sector. It set out supervisory expectations supported by regulatory obligations that firms must adhere to at all times. Risk-based and outcome focused supervision is how we assess both the sector and your firm's adherence to those expectations and regulations. We do this through firm specific, sector wide, and/or thematic engagements. Our 2022 Consumer Protection Outlook Report, which was published in March 2022, also sets out the key cross sectoral risks[2] we identified, which are the primary drivers of risk for consumers of financial services in Ireland and across the EU today. These risks are particularly relevant to the Payment and E-Money sector based on what we have observed over the course of 2022.

Overall, during the last 12 months we have had a further year of intense supervision of the sector. The level of intensity, which is beyond what we would expect for this sector, is on the basis of the significant deficiencies identified in the governance, risk management and control frameworks of some Payment and E-Money firms.

The purpose of this letter is to reaffirm our supervisory expectations built on our supervisory experiences, both firm specific and sector wide, and enhance transparency around our approach to, and judgements around, regulation and supervision. Section 1 of the letter provides wider and specific context to our supervisory approach. Section 2 details key findings from our supervisory engagements over the last 12 months, including outlining a number of actions we expect firms to undertake. Section 3 of the letter sets out our expectation that this letter is provided to and discussed with your Board, and any areas requiring improvement that directly relate to your firm are actioned.

[1] The number of authorised firms having grown by c. 250% since 2018, while users' funds safeguarded have increased by over 700% to €7.56bn by end September 2022.
[2] These risks include poor business practices and weak business processes; the changing operational landscape; technology driven risks to consumer protection; and the impact of shifting business models.

## 1. Supervisory Approach for the Payment and E-Money Sector

The economic environment in which we all operate has materially changed in the last 12 months. The world economy is slowing, with inflation having become more broad-based and persistent. Global financial conditions have tightened amid a pronounced shift in monetary policy, with financial markets in a more vulnerable place, which is evidenced by changes in investor behaviour and higher volatility. There is a heightened uncertainty around the potential source of further shocks. These are key factors contributing to the deterioration in financial stability conditions across the euro area, including in Ireland, as outlined in the ECB's[3] and the Central Bank's[4] recent Financial Stability Reviews. Against this background of a complex and uncertain environment, it is important to reflect and actively consider how we collectively think about and assess risk.

Our approach to the supervision of all financial services sectors is risk-based.[5] The Payment and E-Money sector is no different. Under our approach, the most significant firms, i.e. those with the ability to have the greatest impact on financial stability and consumers, receive a higher level of supervision under structured supervisory engagement plans. Conversely, those firms which have a lower impact are supervised on a sectoral and/or reactive basis. This approach, and our underpinning framework, supports our supervisory engagement with firms, judges the risks they pose, particularly to consumers, assesses the likelihood that risks will actually crystallise and seeks to ensure that the firms we regulate mitigate unacceptable risks.

We have no appetite for the crystallisation of risks that would materially undermine the achievement of our supervisory objectives, which are focused on safeguarding stability and protecting consumers. Where we identify unacceptable or unmanaged risks during the course of our supervisory work, firms can expect supervisory intensity and engagement to increase. This is irrespective of whether a firm is considered high or low impact firm as referred to above. Our supervisory response to such risks is done so in a proportionate manner, leveraging the appropriate regulatory tool from our broad supervisory toolkit; this may include the issuance of a Risk Mitigation programme (RMP), directions and/or enforcement action. Examples of unacceptable risks include; breaches of regulatory requirements, in particular relating to safeguarding and/ or deficiencies in a firm's governance, risk management and internal control frameworks.

We also recognise that the financial services landscape is changing rapidly. Again, the Payment and E-Money sector is no exception. With open banking, digital assets, cross border innovation and expansionary activity, the nature and extent of opportunities and risks are evolving. We recognise that, at times, regulation is challenged by the speed at which the regulatory architecture can move. However, our view is that well-designed rules lead to stronger financial services firms and stronger firms are better able to serve the needs of consumers, households, businesses and the wider economy. The IMF FSAP also identified the need for certain aspects of the regulatory and supervisory framework for Payment and E-Money firms to be strengthened to take account of the changing nature, scale and complexity of the sector. We have actively contributed to the European Banking Authority's (EBA) Call for Advice on PSDII and endorse the proposals put forward by the EBA in this regard. The European Commission is expected to publish a legislative proposal on a new payment services directive in Quarter 2 2023.

[3] European Central Bank Financial Stability Review November 2022
[4] Central Bank of Ireland Financial Stability Review II of 2022
[5] The Probability Risk and Impact System Supervisory Framework (PRISM) underpins how we supervise firms

Against this backdrop, we are seeking to ensure our supervisory strategy and approach for the Payment and E-Money sector remains risk-based, data-driven, intelligence-led and outcomes-focused. We have enhanced our existing engagement structures with sector stakeholders, including regular supervisory engagement with individual firms and listening to the sector's representative bodies. The Financial Services Conference, our Financial Industry Forum and the Retail Payments Forum in particular, have facilitated formal, constructive, and open discussion on issues of strategic importance for financial services in Ireland, including relevant issues for the Payment and E-Money sector.

## 2. Supervisory Findings

As you will be aware, the Payment and E-Money sector is heterogeneous in nature, with a diverse range of business models across the authorised firms. There has been a notable rise in activities being conducted on a pan European freedom of services/freedom of establishment basis by the sector. We continue to see new and innovative technology-driven business models targeting aspects of "traditional" financial services.

We welcome the innovation and competition we are seeing in the sector. Innovation in financial services has the capacity to bring many benefits to consumers and society, and can drive significant growth opportunities for firms. However, to harness the benefits of innovation it must be done well, with risks associated with the innovation appropriately managed and mitigated.

We acknowledge early engagement by a number of firms on planned material changes to their business models, in particular those firms who clearly demonstrate that they have the appropriate governance and risk management frameworks, together with sufficient financial and operational capacity to deliver their proposed business strategy. However, this has not been our consistent experience across all firms operating in the sector. We continue to see examples of firms' strategic ambitions outpacing their frameworks and capacity. Firms are not fully considering the entire suite of financial and non-financial risks they face, including new and emerging risk, particularly in the context of a rapidly changing environment. Moreover, for some firms, our experience has been that regulatory obligations are approached in a tick box manner rather than being adopted as a strategic enabler to enhance business model sustainability, the safety and soundness of the firm and ultimately deliver better consumer outcomes.

The five key areas, outlined below, set out our findings arising from our supervisory engagement over 2022. We have specifically detailed findings, which point to deficiencies identified across key risk areas and our expectations of firms to address them.

### i. Safeguarding

One of the most important objectives for us is that users' funds[6] are protected. As you recall, our December 2021 Dear CEO letter required all firms to complete a comprehensive assessment of their compliance with their safeguarding obligations under Regulation 17 of the European Union (Payment Services) Regulations 2018 (the PSR) and Regulation 29-31 of the European Communities (Electronic Money) Regulations 2011 (as amended) (the EMR). The resultant submissions from the sector, as well as other communications received from firms over the course of 2022, highlighted that **one of every four** Payment and E-Money firms have self-identified deficiencies in their safeguarding risk management frameworks. We acknowledge the efforts of some firms to complete a comprehensive assessment of their safeguarding frameworks, and note the actions being taken to address issues identified. However, in other cases, we received positive attestations from firms that their safeguarding frameworks complied with their

[6] As defined in Regulation 17(1) of the PSR and Regulation 29(1) of the EMR

obligations under the regulations, only to subsequently be advised of the identification of deficiencies in their frameworks. The nature and scale of the safeguarding deficiencies identified indicates that some firms do not have robust safeguarding arrangements in place to demonstrate that users' funds are managed effectively, and protected in accordance with our expectations and obligations under the PSR and EMR. Certain of these safeguarding deficiencies are detailed in Appendix 1. The Central Bank is engaging with firms on an individual basis where specific issues relating to safeguarding have been identified and is requiring timely remedial action to be taken.

We have been clear that there is significant potential for consumer detriment if a firm has not adequately safeguarded users' funds. We have no tolerance for weaknesses in safeguarding arrangements. We expect firms to:

- Have robust, Board approved, safeguarding risk management frameworks in place which ensure that relevant users' funds are appropriately identified, managed and protected on an ongoing basis. This includes the clear segregation, designation and reconciliation of users' funds held on behalf of customer.
- Be proactive in ensuring that the design and operating effectiveness of the firm's safeguarding frameworks is tested on an ongoing basis.
- Notify the Central Bank immediately of any safeguarding issues identified.
- Take mitigating and corrective measures immediately to ensure that users' funds are safeguarded where, in exceptional circumstances, issues are identified.
- Investigate and remediate on a timely basis the underlying root cause of the safeguarding issue(s).

Given the number of issues that have emerged with regard to safeguarding over the last 12 months, this year we are requiring that all Payment and E-Money firms who are required to safeguard users' funds obtain a specific audit of their compliance with the safeguarding requirements under the PSR/EMR. This should be carried out by an audit firm, such as a firm's external auditors. However, we expect firms to exercise due skill, care and diligence in selecting and appointing auditors for this purpose. A firm should satisfy itself that its proposed auditor has, or has access to, appropriate specialist skill in auditing compliance with the safeguarding requirements under the PSR/EMR[7], taking into account the nature, scale and complexity of the firm's business. We expect the auditor to provide an opinion confirming:

- whether the firm has maintained adequate organisational arrangements to enable it to meet the safeguarding provisions of the PSR/EMR on an ongoing basis, with the specific areas, at a minimum, that should be subject to review and assurance by the auditor outlined in Appendix 2.

**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.**

### ii. Governance, Risk Management, Conduct and Culture

We expect firms to be well run with cultures that seek to do the right thing for their consumers. A number of firms in the sector are striving to enhance their governance and risk management capabilities and deliver to the highest standards on an on-going basis. However, this is not being consistently prioritised by all firms and some of the recurring issues we see include:

- Governance, risk management and internal control frameworks not consistently aligned to business strategies and business objectives. For example, instances where firms' business growth runs ahead of their governance, risk management and internal control environment, as measured by business volumes and values, products and services, and distribution channels.

[7] Regulation 17 of the PSR and Regulations 29-31 of the EMR

- Inadequate succession planning, with key positions remaining vacant for a considerable period.
- Inadequate resourcing of the internal audit, risk management and compliance functions leading to poor quality governance of compliance activities and assurance work.
- A focus on achieving minimum compliance, with regulation seen as a cost, rather than as a business enabler to deliver better outcomes for consumers and firms themselves.
- Inadequate reporting to the Board, particularly in relation to customer complaints, fraud levels etc., which can inhibit effective Board oversight of operations and potentially lead to poor outcomes for consumers.
- Product/service disclosures that are unclear and lack transparency, making it difficult for consumers to understand the risks associated with the services they are availing of, who is providing those services (e.g. group affiliates, agents or distributors), and whether or not they are subject to regulatory protections.

We expect firms to consider their governance, risk management and internal control frameworks, in addition to the composition (both number and skills) of their Board and management team, to ensure they are sufficient to run their business from Ireland, as their licenced jurisdiction.

### iii. Business Model, Strategy and Financial Resilience

The Central Bank completed a thematic review of business model and strategic risk (the Review) across a number of firms in the sector during 2022. The Review identified that some firms in the sector do not have defined or embedded Board approved business strategies in place. While firms may operate as part of larger groups, and be reliant on group strategic decisions to inform local strategy, it is critical that robust consideration is given to ensuring there is sufficient financial (capital and liquidity) and operational (resources, IT systems etc.) capacity and capability within the firm to execute that strategy.

It is acknowledged that firms who were subject to the Review are clear on their profitability drivers. However, financial projections and underlying assumptions, including stress scenarios, require further detail to underpin their credibility. We expect firms to have robust strategic and capital planning frameworks which demonstrate that they have a good understanding of the risks that they face and their potential financial impact, such that they can proactively manage their capital to ensure that they are in a position to meet their own funds (capital) requirements[8] on a stand-alone basis at all times, i.e. sufficient regulatory capital is available to absorb losses, including during stress conditions. Furthermore, all firms should have an appropriate exit/wind-up strategy, which is linked to their business model and considers, inter alia, the full return of users' funds in an efficient and timely manner in an exit/wind-up scenario.

Good data, timely and accurate management information are critical to support a firm's strategic and financial planning, and the risk management processes that run and support your business. Weaknesses in risk reporting practices have been identified across a number of firms in the Payment and E-Money sector. Approximately **one of every five firms** in the sector have submitted inaccurate regulatory returns to the Central Bank during the last 12 months. Issues include incorrect methodologies used for calculating own funds requirements; incorrect classification of regulatory capital held; and inaccurate payment values provided.

We expect firms to have Board-approved business strategies in place supported by robust financial projections. Firms must understand and meet their capital requirements at all times[9]. This is particularly

[8] Including Regulation 9 of the PSR and Regulation 14 of the EMR.
[9] Including Regulation 9 of the PSR and Regulation 14 of the EMR.

important given the aforementioned uncertain and complex macroeconomic environment. Strong internal controls must be in place, that are subject to regular testing, to ensure the accuracy and integrity of data used by the firm for regulatory reporting purposes, and for strategic and financial planning.

### iv. Operational Resilience and Outsourcing

Operational Resilience is based on the key premise that operational disruptions will occur. We are increasingly focusing on this and the need for firms to demonstrate readiness for, and resilience to, operational disruptions. As you may be aware, operational resilience is the ability of a firm, and the financial services sector as a whole, to identify and prepare for, respond and adapt to, and recover and learn from an operational disruption. These three pillars underpin our Cross Industry Guidance on Operational Resilience and Cross Industry Guidance on Outsourcing, issued in December 2021, which are applicable to the Payment and E-Money sector.

Technology is at the core of the operations of the majority of Payment and E-Money firms. This reinforces the emphasis required by firms on IT risk management. The foundation of operational resilience is being able to view your business operations through the business service lens. By doing so, your firm can prioritise what is critical or important to your business or the financial system, enabling you to understand the interconnections and interdependencies involved in delivering those services, and therefore assisting in determining the impact a disruption will have on your services.

In the context of our supervisory engagement we have observed an increasing number of major incidents/outages being reported by Payment and E-Money firms. Many of the major incidents/outages reported[10] have been as a result of issues emerging with group/third party providers, who are critical to supporting the IT infrastructure of firms. Ultimate responsibility for a firm's IT risk, strategy and governance rests with executive management of the regulated firm, including the adequacy of digital and IT strategies to deliver and support business strategies and plans. Boards and senior management teams must ensure they themselves have the skills and knowledge to meaningfully understand the risks their firm faces and the responsibilities they have. This responsibility also extends to outsourced activities where the activities are conducted on the firm's behalf by any third party, including any group entity.

Our expectation is that Boards and senior management of Payment and E-Money firms review and adopt appropriate measures to strengthen and improve their operational resilience frameworks in line with the aforementioned Guidance. Given the importance of operational continuity and resilience for the stability of the system and for consumers, businesses and the wider economy, we will continue to challenge how firms are ensuring that risk and control frameworks are operating effectively and are prepared for unforeseen operational disruptions.

### v. Anti-Money Laundering and Countering the Financing of Terrorism

As you are aware, Payment and E-Money firms are classified as designated persons under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (CJA 2010). As a designated person, firms are subject to the obligations of the CJA 2010, and in particular, the obligations set out in Part 4.

[10] Under the major incident or security incident reporting requirements set out in Regulation 119 of the PSR.

Money laundering and terrorist financing divert resources away from economically and socially productive uses and can negatively affect the financial system by undermining its stability and its reputation. Firms should be cognisant of the risk factors[11] which can increase ML/TF risk. These factors include, but are not limited to, high transaction limits, the use of cash to fund transactions and the cross border nature of transactions.

The points below set out observations arising from recent supervisory engagements with the Payment and E-Money sector, and our resulting expectations as to how firms should address these.

- **Risk-Based Approach**

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 ML/TF risks identified. We have found that the risk-based approach employed by some firms in this sector lacks maturity, as outlined in further detail below.

As a consequence of shortcomings in the understanding of ML/TF risk among some firms, controls are not as robust as they should be, and are not commensurate with their level of risk exposure. A particular area of weakness identified relates to the transaction monitoring controls applied by some firms in this sector. Where transaction monitoring controls are not configured correctly, it can lead to a failure to detect suspicious transactions and activity, and/or generate excessive alerts of potential suspicious activity which can impact the timeliness of reporting of suspicions of ML/TF where firms have formed a suspicion of ML/TF.

Further development of the risk-based approach is needed to ensure that there is a more comprehensive understanding as to how the products and services of the firm could be used for ML/TF purposes. AML/CFT controls should be risk sensitive and tailored to the risks identified as part of the ML/TF risk assessment carried out by the firm. For example, transaction monitoring controls should be configured to detect where the ML/TF risks identified as part of the ML/TF risk assessment are materialising.

- **Distribution Channels**

Distributors and agents are a common feature of the Payment and E-Money sector, and they often carry out AML/CFT preventive measures, such as customer due diligence (CDD), on behalf of firms. Weaknesses have been identified, particularly with regard to the oversight of these relationships. Where distributors and agents carry out AML/CFT controls on behalf of firms, it is imperative that this is completed in line with the firms' own ML/TF risk assessment and AML/CFT policies and procedures. It is important that firms recognise that agents and distributors are an extension of the firm itself. We have identified instances where this has not been understood by firms and they have viewed agents and distributors as their customer, despite the fact that they are undertaking activities defined in the legislation on behalf of the firm and under the full and unconditional responsibility of the firm. Where there is an inappropriate level of oversight of the agents and distributors, it can lead to a situation where firms do not have a full

[11] EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions

understanding of the ML/TF risks presented by their actual customers, i.e. those that avail of the products and services.

We expect firms to exercise adequate oversight of the agents and distributors with an appropriate level of ongoing assurance conducted. Firms must undertake appropriate assessment of their agents and distributors that undertake activities on their behalf. 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. However, it is important that firms recognise that the responsibility for carrying out customer risk assessments and CDD on the end user of the products and services ultimately rests with firms, even where such tasks are being performed by agents and distributors.

- **Electronic Money Derogation and Simplified Due Diligence**

Section 33A of the CJA 2010 provides for a CDD derogation for certain e-money products. We have identified some instances of misapplication of this derogation. We have also identified a number of instances where the provisions of Section 34A of the CJA 2010, relating to simplified due diligence, have been misinterpreted by some firms in the sector leading to an incorrect level of CDD applied to customers in those circumstances.

E-Money firms should only avail of the derogation contained in Section 33A in circumstances where it is appropriate to do so and where all the criteria have been met. Firms should be aware that 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.

We expect that simplified due diligence is carried out only where appropriate to do so and where the firm has carried out a risk assessment of each individual relationship, and to do so is justified on the basis of the lower level of risk presented.

## 3. Conclusion and Actions Required

In conclusion, the authorisation and supervision of the Payment and E-Money sector is an important part of the Central Bank's mandate. We are focused on ensuring we strike the balance, which allows the benefits of innovation and growth through this sector to be realised, while ensuring that the risks are managed and mitigated.

The contents of this letter are not intended to provide an exhaustive list of the supervisory findings arising from our supervision of the Payment and E-Money sector. However, these are the areas to which firms can expect the Central Bank to be paying close attention. Firms must not leave aside the identification and management of other potential risks that could lead to consumer detriment or impact their financial and operational soundness.

The Central Bank expects all firms in the sector to discuss this letter with their Board, and to reflect on the supervisory findings called out. Firms should progress the completion of a specific audit of compliance with the safeguarding requirements under the PSR/EMR as outlined in section 2 above, which should be submitted to the Central Bank by **31 July 2023**. We expect firms to take proactive measures to ensure robust and appropriate governance and control arrangements are in place, such that Payment and E-Money firms can grow safely and sustainably, and contribute to the financial ecosystem in a positive way.

In the context of our strategic theme of being 'Open and Engaged' we will continue to engage with firms, and representative bodies of the Payment and E-Money sector, to deepen our own understanding of this evolving sector and enhance transparency around our approach to, and judgements around, regulation and supervision. In addition, we intend to continue to proactively share our supervisory findings to drive enhancements to firms' governance, risk management and internal control frameworks, particularly around safeguarding on a sectoral basis.

If you have any queries on the content of this letter please contact paymentservicessupervision@centralbank.ie.

Yours sincerely

**Mary-Elizabeth McMunn**
**Director of Credit Institutions Supervision**

**Appendix 1: Safeguarding Deficiencies**

- Delays in segregating users' funds following receipt.
- Co-mingling of users' funds and non-users' funds in safeguarding accounts.
- Failing to reconcile that the correct amounts are being segregated on a daily basis.
- Bank accounts where users' funds are held being incorrectly designated and therefore users' funds not safeguarded correctly.
- Failure to maintain adequate insurance policies or comparable guarantees on an ongoing basis, where relevant.
- Control over the safeguarding account resting outside of the firm, for example with a Group entity.
- Insufficient oversight of arrangements for managing the safeguarding of users' funds, for example a lack of policy documentation at the legal entity level (i.e. referable to the Central Bank authorised Payment and E-Money firm) and a lack of effective and regular monitoring and review of safeguarding.
- Consumer Fees/other charges inappropriately taken out of the safeguarding account leading to a potential shortfall of users' funds.
- Failure to evidence adequate consideration of the impact of operational changes, including material changes in the business strategy, on safeguarding arrangements.

**Appendix 2 - Specific Safeguarding Areas that should be subject to Auditor Review**

1. An assessment of the 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. An assessment of the process in place to ensure that users' funds are safeguarded in accordance within the applicable timeframes required under the PSR/EMR[12]. Testing of the process should also be undertaken to provide assurance that these timeframes are being met on an ongoing basis.

3. Confirmation that safeguarding account(s) are appropriately designated (if segregation method of safeguarding is used).

4. An assessment of the appropriateness of the frequency and accuracy of the administration and reconciliation process to ensure there are sufficient users' funds in the firm's designated safeguarding account or to ensure that the insurance policy/ comparable guarantee is sufficient to meet the firm's safeguarding obligations at all times. Testing of the reconciliation process should also be undertaken to provide assurance that the safeguarding reconciliations are being conducted in an accurate and timely manner and that the firm's safeguarding obligation is being met at all times.

5. Where safeguarded funds are invested in secure, liquid and low risk assets or secure and low risk assets, an assessment of the investment policy to ensure the assets chosen are liquid, secure and low risk[13], as the case may be, and that the firm is in a position to manage any market risk associated with this activity.

6. An assessment of the controls over the safeguarding account(s), including the number of persons that have access to the safeguarding account and their functions. Testing of the controls should also be undertaken to provide assurance that these controls are operating effectively on an ongoing basis.

7. An assessment of the Insurance policy/comparable guarantee administration process – including how the firm satisfies itself as to appropriateness of the policy/guarantee, the process for renewing the policy/guarantee, in addition to the process for increasing level of cover where required or making a claim on the policy/guarantee.

8. An assessment of safeguarding breach and incident identification, escalation and management processes including for reporting to the Board/Central Bank.

9. An assessment of whether the liquidity of a firm's safeguarding arrangements facilitates the redemption of e-money at any time and at par value[14] or the timely execution of payment transaction requests.

[12] Per Regulation 17 (2) (a) (ii) of the PSR and Regulation (29 (2) (a) (ii), Regulation 29 (3) and Regulation 30 (2) (a) (ii) of the EMR.
[13] Regulation 17 (2) (a) (ii) of the PSR and Regulation 29 (2) (a) (ii) of the EMR.
[14] Per Regulation 52 (b) of the EMR.