



Strengthening safeguarding for payments and e-money firms in Ireland

Trusted expertise that **adds value**



Introduction

What expectations does the Central Bank of Ireland (Central Bank) have on payments and e-money firms when it comes to safeguarding customer funds? In short, the requirements are set out in two regulations. In addition, the Central Bank has stated, and clarified, its expectations in a series of publications since the key regulations came into effect in Ireland.

This guide sets out specific requirements for firms, and also common safeguarding deficiencies as identified by the Central Bank. Specifically, this guide will cover:

- The importance of safeguarding;
- The safeguarding obligations set out in the regulations;
- Central Bank expectations on firms; and
- Common safeguarding deficiencies.

Contents

- 1 The importance of safeguarding
- 2 The safeguarding obligations set out in the regulations
- 3 Central Bank expectations on firms
- 4 Governance at the first line
- 5 Governance at the second and third line
- 6 Communication with customers
- 7 Common safeguarding deficiencies
- 8 Conclusion



1

The importance of safeguarding

Safeguarding is a means of protecting customer money held with payment service providers (PSPs).

Should a PSP become insolvent, claims of payment service users are paid from the asset pool formed from these funds in priority to all other creditors. Adequate safeguarding measures are a pre-requisite for being granted and retaining Central Bank authorisation for the provision of payments and e-money services.

Firms which are in scope for the safeguarding requirements include authorised payment institutions (PIs), small e-money institutions and authorised e-money institutions (EMIs).



‘User Funds’

Precisely what funds need to be safeguarded varies depending on a firm’s business model (namely, whether the firm is a PI or an EMI). In short, firms must safeguard ‘user funds’. The obligation to safeguard user funds is precise; firms must not safeguard any more, or any less, than funds identified as user funds.

User funds are defined as **customer money, that has either been received by a PI or EMI, for the execution of a payment transaction, or in exchange for e-money that has been issued.**

If at any given time, a firm safeguards less than the user funds it holds, it will be considered to be under safeguarding. Conversely, if a firm safeguards in excess of the user funds it holds, it will be considered to be over safeguarding (or ‘commingling’). Interestingly, both scenarios have been explicitly called out, by regulators, as being inadequate practice.





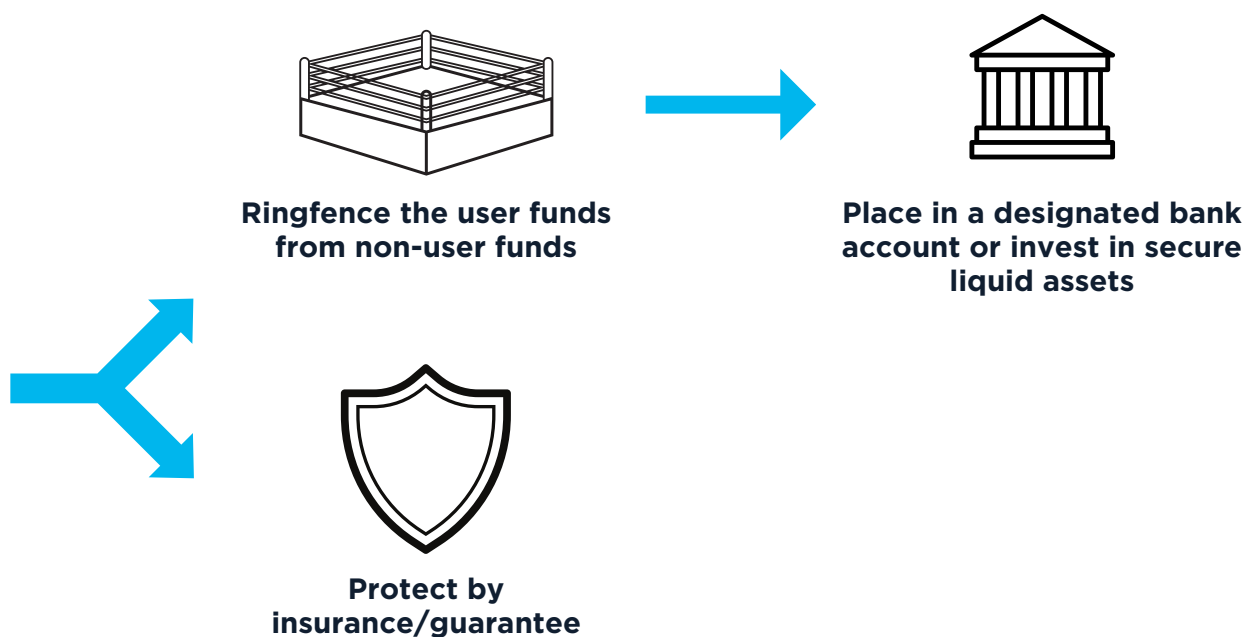
The safeguarding obligations set out in the regulations

In Ireland, there are two key regulations; the European Communities (Electronic Money) Regulations 2011 (the EMRs) and the European Union (Payment Services) Regulations 2018 (the PSRs). The EMRs apply to EMIs and the PSRs apply to PIs.

Methods of safeguarding

Both regulations provide two methods of safeguarding; the 'insurance method' and the 'segregation method'. Firms can safeguard using either method or a combination of both. Due to the costs associated with the insurance method, the segregation method is widely used.

The segregation method involves a physical separation of user funds from non-user funds. Using this method, firms essentially ring fence user funds by removing them from the firm's operational funds environment and either placing them in a special safeguarded bank account or investing them in secure liquid assets.



User funds must be segregated upon receipt and be placed in a specially designated safeguarding account by the end of the business day following receipt. Importantly, the obligation to safeguard user funds continues until the receipt of funds by the end beneficiary.

Reconciliations

The Central Bank expects PSPs to conduct internal and external reconciliations on at least on a daily basis.

- Internal reconciliation: 'what should be safeguarded'. The internal reconciliation compares the internal record of amounts owed to customers in respect of the payment service or e-money (customer liabilities) against the internal record of the aggregate amount of user funds received from customers.
- External reconciliation: 'what in fact is safeguarded'. Once you have obtained assurance as to the amount that should be safeguarded, you should then undertake the external reconciliation. This is a comparison of the aggregate of user funds, per your ledger with the balances held in your safeguarding accounts.



Central Bank expectations on firms

Safeguarding arrangements

In its December 2021 Dear CEO Letter, the Central Bank summarised its expectations on firms as follows:

- Firms must have a Board-approved safeguarding risk management framework in place. This must ensure user funds are identified, managed and protected on an ongoing basis. This should include a daily segregation, designation and reconciliation of user funds;
- Safeguarding arrangements should be reviewed regularly to ensure compliance with the regulations;
- Firms must maintain adequate second and third line functions to provide assurance as to firms' safeguarding frameworks; and
- The Board must seek assurance on an ongoing basis that user funds are fully reconciled and that the calculation of user funds matches with funds held in safeguarding accounts.

In its January 2023 Dear CEO Letter, the Central Bank clarified its expectations on firms as follows:

- Firms must be proactive in ensuring their safeguarding frameworks are effective and test them on an ongoing basis;
- Firms must notify the Central Bank immediately if issues are identified (this is, in fact, a regulatory requirement set out in the EMRs and PSRs);
- Firms must take corrective action immediately to ensure user funds are adequately safeguarded where issues are identified; and
- Firms must investigate and remediate the root causes of any identified safeguarding issues.

Audit requirement

In the 2023 Dear CEO Letter, the Central Bank set out its requirement that all PIs and EMIs obtain an independent audit opinion upon whether or not the firm has adequate organisational arrangements to meet the safeguarding provisions of the PSRs and the EMRs. Key audit focus areas included:

- Governance at the first, second and third line;
- Appropriate designation of safeguarded accounts;
- Performance of reconciliations;
- Controls in place over access to safeguarded accounts; and
- Identification of issues and assessment of breaches.

The deadline for submitting this audit report to the Central Bank was 31 July 2023.



In May 2023, in order to clarify the audit expectations, the Central Bank published a 'Safeguarding Notice'. This stated that firms were required to produce a document (the 'Description') setting out their safeguarding arrangements.



Firms were also required to prepare a Board-approved attestation (the 'Attestation'). The Attestation should state whether the Description is fair and that the controls described within are operating.



Finally, firms were required to engage an auditor to perform a further attestation (the 'Reasonable Assurance Attestation'). The auditor's conclusion should be expressed in a positive form as to whether, in their opinion, the firm's Description is fairly presented to enable the firm to make the Attestation.

The Reasonable Assurance Attestation, however, does not provide assurance on whether the arrangements described are appropriately designed to comply with the safeguarding requirements in the EMRs and PSRs.

4



Governance at the first line

All firms will take a slightly different approach in terms of governance depending upon the size of their firm and the resources available. That being said, there are some key things the Central Bank expects to see from a governance perspective.

Safeguarding policy

The safeguarding policy should receive Board approval and should be updated annually and more regularly in light of business and regulatory change. The policy should be sufficiently detailed to set out the firm's systems and controls with regards safeguarding. Below is a non-exhaustive list of information to be set out in the firm's safeguarding policy:

- Internal roles and responsibilities, including escalation routes and a description of lines of defence;
- A definition of 'business days';
- Details of the firm's safeguarding provider and the specific safeguarded accounts held;
- The firm's funds flow;
- The treatment of unallocated funds;
- A rationale for the frequency of reconciliations;
- Details on how discrepancies are dealt with during reconciliations;
- Details of the firm's risk assessment and associated monitoring conducted; and
- Details of the firm's breach register and processes for reporting externally to the Central Bank.

Safeguarding acknowledgement letter(s)

Firms must hold safeguarding acknowledgement letters from an authorised credit institution (they cannot be held with another EMI or PI). The acknowledgement letters must be signed and dated and must specifically refer to the relevant designated safeguarded accounts in which user funds are held.

Reconciliations procedure

Firms must have a reconciliations procedure that is sufficiently detailed and shows (in step-by-step format) the reconciliation process including the details of those from whom sign-off is required and matters are escalated to.

Reconciliation records

Firms must keep a record of each reconciliation conducted and requisite sign-off from a member of senior management. The reconciliation records should evidence the full investigation of any discrepancies discovered for record keeping purposes.

Safeguarding training

Firms should ensure that all employees are aware of the safeguarding obligations. Training should be provided to employees upon commencement of employment and annually thereafter.

Training should be refreshed periodically and should be informed by horizon scanning to remain up to date with regulatory developments and updates from the Central Bank.



Risk register

Firms should maintain a detailed risk register which firstly sets out the firm's risk appetite regarding safeguarding risks. The risk register should set out at a granular level, specific inherent safeguarding risks, the controls that the firm has in place to mitigate them, and the residual risk score upon application of controls. Key risks to be considered include, but are not limited to, the following.

- The risk that reconciliations are not undertaken on a daily basis;
- The risk that reconciliations or any resulting transfers do not receive requisite sign off;
- The risks that employees are not adequately aware of the firm's safeguarding obligations; and
- The risk that the firm has not developed sufficient organisational arrangements to ensure the adequate protection of user funds.

Risk assessment of banking counterparty

Firms should ensure to risk assess their banking counterparty with which safeguarded accounts are opened. Once assessed, firms should review their counterparty, assessing suitability and longevity on an ongoing basis, with the assessment being undertaken on a rolling annual basis.

Evidence of Board oversight and awareness

Boards should meet at a set cadence and do so more often in light of regulatory or business change. It is recommended that safeguarding is a set agenda item at Board meetings and that formalised minutes are recorded. The same principles apply to any further committees related to safeguarding.



5

Governance at the second and third line

Second line

Firms must ensure there is a clear distinction between the first and second lines of defence.

Firms must ensure they have an adaptable (and real time) compliance monitoring plan proportionate to the nature, scale, and stage of the business, that clearly sets out for the entire year the monitoring to be undertaken with regard to safeguarding. This should, at a minimum, include reference to the following:

- The specific tests to be undertaken;
- The individual responsible for ensuring the monitoring activities are adhered to;
- The dates at which certain monitoring activities are to be conducted;
- The status, and outcomes, of each monitoring activity;
- Whether all planned monitoring has been completed;
- Set sample sizes for testing;
- Established metrics for success and failure; and
- Remedial actions and their progress.

Third line

The third line of defence is that of an audit function. This may either be performed by an internal or external auditor (the results of which should be shared with and reviewed by the Board).



6

Communication with customers

Firms should ensure that communication with customers is clear and unambiguous. Terms and conditions should state that the firm is not itself a bank and that customer funds are safeguarded in bank accounts separate from the firm's own funds. As such, while customers may not avail of protection from the Deposit Guarantee Scheme, their funds are protected under safeguarding rules.



Common safeguarding deficiencies

In its January 2023 Dear CEO Letter, the Central Bank revealed that one in four PSPs had identified deficiencies in their safeguarding risk management frameworks. In response, the Central Bank set out specific safeguarding deficiencies it had encountered in its regulatory capacity as follows:

1. *Delays in segregating user funds following receipt:* the requirement to segregate user funds is, in fact, immediate;
2. *Commingling of user and non-user funds:* in the event of insolvency this would lead to difficulty in identifying and returning user funds;
3. *Failure to reconcile on a daily basis:* the Central Bank expects a daily internal and external reconciliation to occur, to be correct, to be signed off and be recorded for record keeping purposes;
4. *Incorrectly designated bank accounts:* accounts used to hold safeguarded funds should be explicitly named as safeguarded bank accounts;
5. *Insufficient oversight and monitoring:* firms must ensure that the second line assurance function adequately tests the firm's systems and controls on a regular basis as informed by the risks identified in the firm's risk assessment; and
6. *Lack of consideration of operational changes on safeguarding arrangements:* operational changes should be risk assessed to ensure continued compliance with the safeguarding requirements. If, for example, a firm decides to outsource a function affecting safeguarding, this must be risk assessed, and effective oversight should be maintained.



8

Conclusion

Safeguarding customer (user) funds is a fundamental regulatory requirement for payments and e-money firms operating in Ireland. The Central Bank, by way of its supervisory guidance, has set out its expectations that robust safeguarding arrangements are maintained.

The Central Bank's continued focus on this area underscores the importance of maintaining high safeguarding standards. Ultimately, firms must treat safeguarding as an ongoing priority rather than a one-time compliance exercise. By embedding safeguarding principles within risk management frameworks and corporate governance structures, firms can ensure regulatory compliance, protect customer funds, and contribute to the integrity and stability of the payments and e-money sector in Ireland.

Our experts



Philip Creed

Head of Europe Consulting

philip.creed@fsc.com.co



Matt Allen

Safeguarding Expert

matt.allen@fsc.com.co




Richard Dunlop

Safeguarding Expert

richard.dunlop@fsc.com.co

Have a compliance question?

 +353 (1) 640 1986

 info@fscom.co

 fscom.co

 +44 (0) 28 9042 5451

 [@fscom1](https://twitter.com/fscom1)

 [@fscom-limited](https://www.linkedin.com/company/fscom-limited)

