



# Safeguarding arrangements of non-bank payment service providers

---

In the first 6 months of 2019 we carried out a multi-firm review with 11 non-bank payment service providers (PSPs) to assess how well they meet the requirements for safeguarding service users' funds in the Payment Services Regulations 2017 (PSRs) and Electronic Money Regulations 2011 (EMRs) (the Regulations). These are our key findings.

---

The Regulations ensure that PSPs protect customer funds by creating a segregated asset pool of relevant funds from which to pay the claims of electronic money (e-money) holders or payment service users in priority to other creditors if the PSP becomes insolvent.

Our review into authorised payment and electronic money institutions identified both positive and negative practices in the ways in which these institutions sought to comply. We have outlined some of the practices we observed here.

While this report is based on observations from a small sample of firms, the findings are relevant to other non-bank PSPs. We encourage all these firms to consider our findings and how they apply to their own organisations. Institutions should consider the [guidance in our Approach Document](#) [1] and may want to seek their own legal advice about whether their arrangements comply with the Regulations and effectively safeguard customer funds.

## Findings

### How well firms understood which funds are relevant funds

The PSRs define relevant funds as (a) sums received from, or for the benefit of, a payment service user for the execution of a payment transaction, and (b) sums received from a payment service provider for the execution of a payment transaction on behalf of a payment service user. In the EMRs they are defined as funds that have been received in exchange for electronic money that has been issued.

To be able to safeguard relevant funds properly, firms must first determine how the Regulations apply to their activities and product offerings.

Our review showed that, when identifying relevant funds, most firms understood which payment services they provided and when they were providing them.

However, some firms were unable to explain which payment services they provided in certain situations or identify when they were issuing e-money, nor was there clarity about when they were acting as agent or distributor for another payment service provider. This meant that they could not accurately identify relevant funds and did not know whether they were safeguarding the correct amount of relevant funds.

### Effectiveness of firms' safeguarding procedures and documentation

We expect institutions to maintain records that are sufficient to show and explain their compliance with all aspects of their safeguarding obligations. We expect them to have a documented rationale for every decision they make about their safeguarding process and the systems and controls they have in place.

We found that firms that had documented their rationale for safeguarding decisions were generally more likely to be safeguarding appropriately.

Some firms provided a clearly documented rationale for their safeguarding methods, systems and controls to effectively safeguard relevant funds in practice and their documentation named an individual with responsibility for overseeing all safeguarding procedures. These firms regularly updated these documents when they made relevant decisions and recorded the outcomes appropriately.

But others did not have up to date safeguarding policies or equivalent documentation in place at the time of our review. Some relied on operational process documents which either did not include the rationale for the arrangements or simply reiterated the Regulations and guidance without explaining how their systems and controls would ensure compliance with them.

## How well firms met our expectations on segregating funds

The obligation on firms to safeguard starts as soon as they receive relevant funds. For firms using the segregation method, funds must be segregated upon receipt. If relevant funds continue to be held at the end of the business day following the day of receipt, the firm must:

- deposit relevant funds in a separate account that it holds with an authorised credit institution or the Bank of England, or
- invest the relevant funds in secure, liquid assets approved by us and place those assets in a separate account with an authorised custodian

We expect institutions to segregate relevant funds by receiving them into a separate account. Where, for customer convenience, any other funds are paid into the account they should be removed as frequently as practicable throughout the day. Other sources of funds include fees and collateral for foreign exchange transactions. In no circumstances should such funds be kept together overnight.

We found that some firms received relevant funds and other sources of funds into separate accounts, which means that they were segregated on receipt. One firm which received fees and relevant funds into the same account did remove the fees as frequently as practicable throughout the day.

But others did not attempt to segregate relevant funds on receipt. There were instances where relevant funds were received into accounts with funds held for other purposes. Very few firms removed other sources of funds more than once a day.

## How effectively agents and distributors were overseen

Where relevant funds are held on a firm's behalf by agents or distributors, the firm remains responsible for ensuring that the agent or distributor segregates the funds. Firms should have arrangements in place to ensure that relevant funds held by agents or distributors are safeguarded as soon as they are received.

Institutions may also choose to segregate an equivalent sum to the relevant funds received by their agents or distributors.

We found that one business segregated relevant funds upon receipt by agents or distributors by maintaining an equivalent sum in a separate segregated account to reduce the risk to other safeguarded relevant funds.

However, other firms which received relevant funds through agents or distributors did not take any measures to ensure that they were segregated on receipt. These firms calculated their safeguarding obligation at the end of the business day on which e-money was issued and transferred into a safeguarding account the next business day. This meant that relevant funds were combined with other non-relevant funds overnight.

## Designating safeguarding accounts

Accounts in which relevant funds or assets are placed must be designated in a way that shows it is a safeguarding account. If it is not possible for an European Economic Area (EEA)-authorised credit institution to make this designation evident in the name, we expect e-money and payment institutions to provide evidence, such as a letter, confirming the appropriate designation. No person other than the institution may have any interest in or right over the relevant funds or the relevant assets in these accounts.

Our review showed that some firms could evidence appropriate account designations for all the safeguarding accounts they held.

But we also found that for several firms the account designations were not clear. Instead, the accounts were named according to their operational function or after the relevant agent or distributor.

## How effectively firms carried out reconciliations

An institution should carry out internal and external reconciliations as often as necessary, considering the risks to which the business is exposed. It should support its approach to reconciliation with a clear explanation, which must be signed off by its board of directors.

Where there is the potential for discrepancies between the balance in the safeguarding account, and the amount that should be safeguarded, the firm should carry out reconciliation as often as is practicable. In no circumstances would it be acceptable for a firm to carry reconciliation less than once during each business day. The reconciliation should result in the amount of funds or assets safeguarded being:

- sufficient to cover the amount that the institution would need to safeguard before the next reconciliation, and
- not excessive – to minimise risks from commingling

We found that some firms carried out reconciliations at least daily and adjusted the balance immediately where they identified discrepancies. Their procedures were supported by a clear explanation signed off by the board of directors and they had a periodic review process in place. One firm had automated controls to remove other sources of funds frequently throughout the day.

But several institutions either did not carry out both internal and external reconciliations, did so infrequently or did not adjust the balance of their safeguarded accounts in a timely way when they identified discrepancies. This resulted in the commingling of funds overnight, as the institutions relied on the results of their reconciliations to manually withdraw excess sums from safeguarding accounts.

## The effectiveness of firms' governance and oversight arrangements

Institutions' organisational arrangements must be sufficient to minimise the risk of the loss or diminution of relevant funds or assets through fraud, misuse, negligence or poor administration (regulation 24(3) of the EMRs and regulation 23(17) of the PSRs 2017). This requirement is in addition to the general requirements on institutions to have effective risk management procedures, adequate internal control mechanisms and to maintain relevant records. They should monitor these procedures through robust governance arrangements.

Our review found some firms monitored safeguarding risks on an ongoing basis, gathering suitable management information on safeguarding issues for presentation to governance forums at regular intervals. This ensured that the rules were consistently applied to new product offerings as their business developed over time. In some cases, staff were continually trained on safeguarding issues.

But other firms considered safeguarding risk only on an exceptions basis and would only revisit their processes if they identified a breach. In some of these cases, their controls to identify a safeguarding breach were not fit for purpose. This meant that these firms did not adequately consider safeguarding when developing new products, leading to inadequate safeguarding processes.

## Main observations from our findings

The main aim of the review was to assess how well non-bank PSPs met the requirements to safeguard customer funds in practice and whether e-money holders and payment service users may suffer financial loss or other harm if a firm fails.

We found examples where firms were meeting the individual components of the requirements effectively, but others where further work was needed to ensure customers' funds were fully protected if the firm became insolvent.

- Some firms need to be clearer about how their business models work and which funds are relevant and should be safeguarded.
- Some firms were not segregating relevant funds on receipt. These firms need to ensure that relevant funds are segregated as quickly as possible when they receive them.
- The checks we saw to ensure the correct amounts are being safeguarded were not always as frequent or accurate as they should be.
- In some cases, firms with networks of agents or distributors did not have adequate processes to ensure that relevant funds are segregated on receipt.
- Firms need to ensure they have sufficient oversight of their arrangements for managing the risks to customer funds. This includes sufficient detail and rationale in their documentation and regular, effective monitoring and review of safeguarding processes. This is particularly relevant where firms have rapidly evolving business and operating models.

## Next steps

On 4 July 2019, we published a [Dear CEO letter requiring all electronic money institutions and authorised payment institutions to review their safeguarding arrangements](#) [2], to make sure they fully meet the requirements.

These firms should attest to the FCA that they are satisfied that they meet the requirements by 31 July 2019.

We will be conducting further work on firms' safeguarding arrangements, and expect to see that firms have acted to review and where necessary remediate their processes. Where we find inadequacies in firms' safeguarding we will take appropriate action.

**Source URL:** <https://www.fca.org.uk/publications/multi-firm-reviews/safeguarding-arrangements-non-bank-payment-service-providers>

Multi-firm reviews | First published: 04/07/2019 | Last updated: 04/07/2019

---

## Links

- [1] <https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf>
  - [2] <https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-non-bank-payment-service-providers-requirements-for-safeguarding-of-customer-funds.pdf>
  - [3] <https://www.fca.org.uk/print/publications/multi-firm-reviews/safeguarding-arrangements-non-bank-payment-service-providers>
  - [4] <https://www.fca.org.uk/publications/multi-firm-reviews/safeguarding-arrangements-non-bank-payment-service-providers>
  - [5] <https://www.fca.org.uk/publication/forms/safeguarding-attestation-authorised-payment-institutions.pdf>
  - [6] <https://www.fca.org.uk/publication/forms/safeguarding-attestation-electronic-money-institutions.pdf>
- 

## Safeguarding arrangements of non-bank payment service providers [5]

### Related information

Dear CEO letter: non-bank payment service providers	[2]
Safeguarding attestation: authorised payment institutions	[6]
Safeguarding attestation: electronic money institutions	[7]

### Request an alternative format

Call 020 7066 7948, email [8] or write to Editorial and Digital team, Financial Conduct Authority, 12 Endeavour Square, London E20 1JN

---