Safeguarding Good Practice Guidance

Updated March 2026

THE ASSOCIATION OF FOREIGN EXCHANGE AND PAYMENT COMPANIES

About AFEP

Founded in 2012, AFEP serves as the representative body for firms providing foreign exchange and payment services, including Authorised Payment Institutions, Electronic Money Institutions, and MiFID-regulated foreign exchange firms.

Our mission is to raise standards across the FX and e-money sector and to advocate effectively on behalf of our members with regulators and government bodies.

The AFEP Risk and Compliance Executive Committee develops and oversees industry Good Practice Guidance on key regulatory and operational topics. This guidance supplements the FCA's rules by clarifying expectations and promoting standards that are specific to the FX, e-money and payment services sector.
These Good Practice Guidance documents play a significant role in shaping how firms within our industry are expected to operate in practice.

AFEP recognises the importance of members not only adhering to the FCA rules and regulations but also these Good Practice Guidance documents. Member firms are required, as a condition of membership, to adhere to the Good Practice Guidance.

Background

This Good Practice Guidance relates to the requirement for payment services firms to safeguard funds received from payment service users for the execution of payment transactions. This is high-level guidance, as each firm is responsible for determining how the safeguarding requirements apply to its specific business model. This guidance is intended for Authorised Payment Institutions (API's) and Authorised Electronic Money Institutions (EMI's) who are full members of AFEP.

The legislative framework governing safeguarding requirements for payment services firms are set out in the Payment Services Regulations 2017 (the "PSRs") and the Electronic Money Regulations 2011 (the "EMRs") respectively.

In addition, the FCA provides supervisory guidance in Chapter 10 of "Payment Services and Electronic Money – Our Approach. The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011" (the "FCA Approach document").

From May 2026, firms must comply with the FCA's safeguarding framework set out in CASS 15 (Client Assets Sourcebook: Safeguarding). Firms must also comply with relevant provisions within SUP concerning audit requirements, regulatory reporting and notification obligations relating to safeguarding.

Where a firm also holds MiFID investment permissions and is subject to CASS 7 (Client Money), the interaction provisions in CASS 10A (Resolution Pack) must also be considered.

Firms should ensure they understand how these rules apply to their individual permissions and business models, including any overlapping obligations arising from other regulated activities.

In addition to the legislative and handbook requirements, recent insolvencies, enforcement action and case law have clarified regulatory expectations regarding safeguarding controls and governance. The below may help firms better understand the FCA's expectations and the rationale for some of the regulatory changes:

- Premier FX Final Notice - https://www.fca.org.uk/publication/final-notices/premier-fx.pdf
- IPAGOO - *Ipagoo LLP (in administration) [2021] EWHC 2163 (Ch)*
- Barclays Fine in relation to Premier FX - https://www.fca.org.uk/publication/final-notices/barclays-bank-plc-2022.pdf
- Press articles and administrators' reports for recent insolvencies including
    - Rational Foreign Exchange
    - Guavapay Limited
    - Argentex LLP
-

1. Oversight and Governance

Clearly defined oversight and governance in respect of safeguarding requirements are key in ensuring that customer funds are adequately protected, and risks are correctly identified. AFEP has issued separate guidance on Corporate Governance and we do not seek to duplicate this in this document but have set out below the key areas we believe may have an impact on safeguarding and some of the considerations that should be applied by member firms.

Firms should note that under CASS 15, a director or senior manager must be formally appointed with responsibility for oversight of compliance with the safeguarding requirements. This individual must have sufficient authority, expertise and independence to oversee safeguarding arrangements and must report directly to the firm's governing body. For smaller firms, this role may be fulfilled by an appropriately senior manager, provided there is clear accountability and direct reporting to the governing body.

1.1 Three Lines of Defence

Firms should ensure safeguarding governance operates within a Three Lines of Defence model:

- **First Line – Business Operations**
Operational teams responsible for payments processing, treasury management, reconciliations and safeguarding calculations are responsible for executing safeguarding controls and maintaining accurate records.

- **Second Line – Risk and Compliance**
Risk and Compliance functions provide independent oversight and challenge of safeguarding arrangements, including review of safeguarding calculations, reconciliation processes, data sources and regulatory reporting.

- **Third Line – Internal and External Audit**
Internal and external audit should provide periodic independent assurance over the effectiveness of safeguarding governance, internal controls, reconciliation processes and regulatory compliance.

Under the FCA's new safeguarding framework, safeguarding audits for firms holding more than £100,000 in relevant funds must be conducted by statutory auditors. Auditors will be required to report all safeguarding breaches directly to the FCA, regardless of materiality. This removes discretion from senior management and strengthens transparency obligations.

This structure supports appropriate segregation of duties and ensures safeguarding controls are subject to independent challenge and assurance.

1.1 Board Oversight and Accountability

1.1 Purpose
Under the safeguarding framework set out in CASS 15, firms are required to maintain robust governance arrangements and effective oversight of safeguarding systems and controls. Ultimate responsibility for compliance rests with the Board.
This section provides guidance on the matters the Board should actively oversee and the challenge questions Directors should consider to ensure the firm meets its safeguarding obligations

1.2 Board Responsibilities

The Board should ensure that:

- The firm has a clearly documented safeguarding framework aligned to CASS 15.
- Roles and responsibilities for safeguarding are clearly defined and understood.
- Safeguarding calculations and reconciliations are performed accurately and on a timely basis.
- Safeguarding accounts are appropriately structured and legally protected.
- Appropriate escalation and regulatory notification procedures are in place.
- The firm maintains a compliant Client Assets and Safeguarding Record (CASR) / Client Money and Asset Record (where applicable).
- The firm conducts annual reviews of safeguarding arrangements and audit effectiveness.
- Safeguarding risks are integrated into the firm's broader enterprise risk management framework.

The Board should receive regular MI sufficient to discharge these responsibilities.

1.3 Board Challenge Questions
Directors should be able to answer the following:
Governance and Accountability

- Who is the designated senior individual accountable for safeguarding?
- How is safeguarding oversight evidenced at Board level?
- When was the safeguarding framework last formally reviewed?

Calculations and Reconciliations

- Are safeguarding calculations performed daily (or at required frequency)?
- How do we evidence that reconciliations are complete and independently reviewed?
- Have any reconciliation breaks occurred in the last 12 months? If so, how were they resolved?

Banking and Insurance Arrangements

- Are safeguarding accounts clearly segregated and legally protected?
- Where insurance or guarantee is used, how has compliance with CASS 15 been independently verified?
- Have acknowledgment letters been reviewed for compliance with FCA requirements?

Hybrid Firms (CASS 7 and CASS 15)

- Are client money and safeguarded funds held in separate accounts?
- Are reconciliations and reporting processes clearly separated in accordance with CASS 10A interaction provisions?

- How do we ensure no operational co-mingling occurs?

Regulatory Reporting and Notifications

- How do we ensure Monthly Safeguarding Return data aligns with safeguarding calculations?
- Have any safeguarding breaches been notified to the FCA?
- Are escalation triggers clearly documented?

Third Parties and Agents

- What due diligence is performed on safeguarding banks?
- How often are safeguarding arrangements reassessed?
- How are agents monitored to ensure safeguarding compliance?

Resolution Planning

- When was the Client Assets and Safeguarding Record last reviewed and tested?
- Could the record be provided to an insolvency practitioner within 48 hours?

1.4 Annual Board Safeguarding Attestation Checklist

At least annually, the Board should formally confirm that:

☐ The firm complies with safeguarding requirements under the PSRs / EMRs and CASS 15
☐ Safeguarding calculations and reconciliations are operating effectively
☐ Safeguarding accounts remain appropriately designated and protected
☐ The firm has assessed safeguarding bank diversification and concentration risk
☐ Acknowledgment letters meet regulatory expectations
☐ Regulatory reporting (including Monthly Safeguarding Return) is accurate and reconciled
☐ The CASR / safeguarding record is complete and up to date
☐ No unreported safeguarding breaches have occurred
☐ A Safeguarding auditor has been appointed and the audit undertaken
☐ Internal audit / external audit findings have been appropriately addressed
☐ Safeguarding remains adequately resourced and supported

This attestation should be minuted and retained as part of the firm's governance record

1.1 Key risks

Failure to ensure that robust oversight and governance structures are in place may result in customer funds not being adequately safeguarded. Additionally, as safeguarding is a key area of focus for Firms banking counterparties, risk of not complying with safeguarding requirements could result in de-risking of this sector by the banking sector.

Failure to have a good oversight and governance controls, is a breach of Principle 11, where Firms should ensure they are clear and transparent with the FCA on any regulatory issues arising within the Firm, which includes safeguarding.

1.2 Guidance

We expect all member firms to:

a) adhere to AFEP's Safeguarding good practice guidance;
b) formally appoint a director or senior manager with responsibility for safeguarding compliance in accordance with CASS 15. This individual must have clearly documented responsibilities and sufficient authority to oversee safeguarding arrangements. Clear lines of responsibility should be documented from the governing body to operational delivery. Depending on the size and complexity of a Firm's operations, a regular Safeguarding or Client Money Committee should be considered to discuss safeguarding issues on a periodic basis;
c) explicitly consider the requirement to safeguard funds and consider how it applies to their business and the products and services offered to ensure total capture;
d) conduct and document a diversification assessment in respect of safeguarding counterparties. Firms should assess, based on the due diligence performed on each safeguarding bank or insurance provider, whether concentration risk exists and what triggers would necessitate the appointment of more than one safeguarding counterparty. This assessment should consider credit risk, operational resilience, jurisdictional risk and access to funds in insolvency. The same principles should be applied to insurance-based safeguarding arrangements;
e) establish and maintain a documented CASS 15 rule mapping and control mapping framework. Firms should identify all applicable safeguarding rules and map these to documented policies, procedures and controls. It is essential that end-to-end fund flows are clearly documented to support the framework.
f) A formal safeguarding gap assessment and risk matrix should be maintained, identifying control owners, inherent and residual risks, remediation actions and review frequency. In preparation for the changes it is recommended that firms have a formal 'readiness' check recorded and any areas of remediation or risk are addressed and monitored. Policies and procedures should be derived from this mapping exercise and reviewed at least annually or following material change;
g) The firm maintains a documented safeguarding risk management framework covering operational, liquidity, counterparty, FX, reconciliation and third-party risks associated with safeguarding.
h) Firms should ensure that safeguarding counterparty concentration risk, FX-related safeguarding treatment, and agent responsibility boundaries are subject to periodic Board review and formally recorded in meeting minutes.
i) provide sufficient and regular MI to the governing body and the appointed safeguarding responsible individual to enable effective oversight of the firm's safeguarding arrangements and the effectiveness of associated controls;
j) Comply with the mandatory annual safeguarding audit requirement under CASS 15. The audit must be undertaken by an external auditor with appropriate safeguarding and CASS expertise. The governing body

should formally assess and document the auditor's competence, experience and independence. Independent review should also be triggered following any material change to the safeguarding model, client product set, payment channels or delivery channels;

k) Ensure the governing body conducts and formally documents at least an annual review of the firm's safeguarding arrangements, including review of the safeguarding policy, reconciliation methodology, CASS Resolution Pack (CRP) completeness, diversification assessment, audit findings and breach register. The governing body should formally attest that safeguarding arrangements remain appropriate for the firm's business model.
l) Put in place robust processes for breach identification, recording escalation and regulatory reporting in accordance with SUP notification requirements;
m) Ensure clients receive sufficient information to understand what funds are and are not safeguarded. Communication with customers relating to the safety of their funds must be clear, fair and not misleading. Such communication should not be promotional in nature as all firms are required to meet the regulatory requirements;
n) Ensure staff with safeguarding responsibilities at the firm are adequately trained ensuring they understand their regulatory responsibilities and are able to perform their functions accordingly; and,
o) Where a firm has agents or introducers:

    - ensure all communications clearly explain the safeguarding protections applicable to customer funds, in line with Consumer Duty obligations;
    - clearly document and disclose when safeguarding responsibility begins and ends, including identification of any operational or timing gaps;
    - ensure contractual arrangements make clear that agents do not hold or control client funds unless expressly permitted and appropriately safeguarded;
    - where collateral is provided by agents, assess and document how this interacts with safeguarding obligations and ensure there is no customer detriment arising from ambiguity in responsibility;
    - Firms should ensure that all communication is clear in respect of the client money protection offered.
    - Agents should be monitored and undergo periodic reviews to monitor compliance with a Firms safeguarding controls.

	Good practice	Poor practice
1	Clearly documented oversight framework including: • formal appointment of a director or senior manager responsible for oversight of operational compliance with safeguarding under CASS 15 and reporting to the governing body; • documented CASS rule mapping and control matrix; • safeguarding risk assessment and gap analysis commensurate with the size and nature of the business	Lack of documented governance framework and/or one that is documented but not implemented in practice.
2	Director or Senior Manager explicitly appointed with responsibility for safeguarding under CASS 15, with documented role description and regular Board reporting.	Lack of defined safeguarding responsibility at Board level or unclear accountability framework.
3	Clearly documented Safeguarding Policy commensurate with the size and nature of the business approved by Board, including identification of relevant funds. Safeguarding Policy and identification of funds is updated to reflect new business products and processes.	• Lack of documented Safeguarding Policy and/or one that is documented but not implemented in practice. • No evidence of Board approval.
4	Clearly documented roles and responsibilities for safeguarding processes and procedures, accepted by relevant staff confirming their understanding and acceptance of those responsibilities. For Large Firms, a designated Committee for Safeguarding purposes, or a	Lack of or ill-defined responsibilities and/or gaps/overlap in areas of responsibility.

	standing agenda item for regular Executive Meetings.	
5	Clear policy for breach recording and reporting, breaches escalation process and reporting threshold to the regulator.	Failure to identify, record or report breaches
6	Regular MI presented to the governing body and the safeguarding responsible individual including: • amounts safeguarded and reconciliation outcomes; • whether safeguarded balances are aligned with regulatory capital requirements; • safeguarding counterparties used (banks/insurers), including diversification assessment and concentration exposure; • summary of due diligence performed on safeguarding counterparties; • breaches identified and remediation status (including regulatory notifications made); • findings from independent safeguarding audits; • findings from internal audit or compliance monitoring reviews relating to safeguarding; • relevant regulatory communications concerning safeguarding (whether firm-specific or sector-wide) and the firm's impact assessment; • data reported in regulatory returns including, where applicable, information required under the Monthly Safeguarding Return (from May 2026); • staff training and competency metrics.	Failure to provide adequate MI to permit the board to understand safeguarding processes and requirements

7	Mandatory annual safeguarding audit conducted by an appropriately skilled and independent external auditor. The governing body formally assesses and documents auditor competence and independence. Audit findings are tracked to remediation and reported to the governing body with clear accountability and timelines.	Internal reviews performed by staff involved in administering safeguarding policy and processes, or failure to comply with the mandatory safeguarding audit requirement.
8	Where funds are received in connection with a payment instruction that includes an FX transaction, the firm has: • clearly documented whether the transaction constitutes a first-party transfer or payment to a third party; • documented its rationale for the safeguarding treatment applied; • established and documented how it distinguishes between funds pending FX settlement and funds subject to safeguarding requirements; • ensured transparency to customers where funds may not be safeguarded during part of the FX settlement process; • reviewed its approach in light of updated FCA expectations and documented Board approval of the treatment.	Failure to distinguish between FX settlement funds and safeguarded funds, lack of documented rationale, or lack of transparency to customers regarding protection status.

2. Relevant funds

The requirement to safeguard applies to 'relevant funds' in both the PSRs and EMRs.

All authorised APIs are required to comply with the safeguarding requirements in regulation 23 of the PSRs, where relevant funds are defined as:

- sums received from, or for the benefit of, a payment service user for the execution of a payment transaction; and
- sums received from a payment service provider (PSP) for the execution of a payment transaction on behalf of a payment service user.

All AEMIs are required by regulation 20 of the EMRs to safeguard funds received in exchange for e-money that has been issued. Where an AEMI provides unrelated payment services, it is required to comply with the safeguarding requirements in regulation 23 of the PSRs above.

For an E-Money firm, relevant funds are defined as "funds of the e-money users against which they have a claim." This means, any funds received on behalf of the client, against which e-money is issued, is deemed as "relevant funds." For e-money firm who offer FX, Firms should evaluate whether they are offering immediate delivery of the FX or not and what impact this will have on safeguarding obligations.

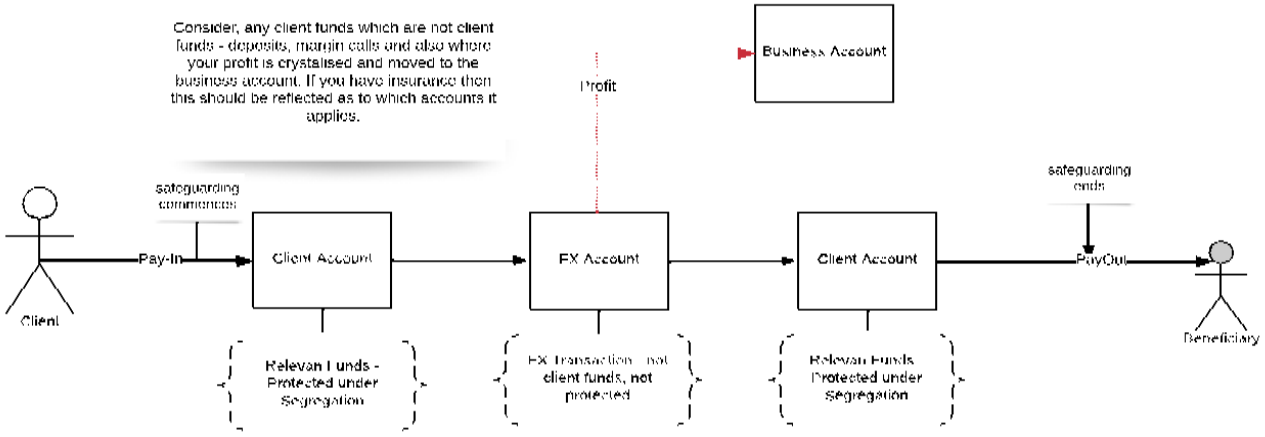

Figure 1: Example Flow of Funds Diagram (this will be different for individual firms)

2.1 Key risks

Failure to correctly define and identify relevant funds, including where payments are combined with FX services, fees, margin, deposits or other linked products, may result in significant customer detriment in the event of the insolvency of an API or AEMI

Failure to properly document how fees are collected (for example, via invoice-based models), the account into which they are received, and whether they form part of the safeguarding requirement, may result in co-mingling or incorrect exclusion from the safeguarding pool.

2.2 Guidance

We expect all member firms to:

a) identify and define relevant funds in relation to their business model, including:
   - treatment of first party FX settlement payments;
   - "two leg out" transactions;
   - linked products working alongside the payment (including FX conversion, margin, forward contracts, fees and commission);
   - how and where fees are received (including invoice-based collection models), and into which account such funds are credited;

b) identify and clearly define when the safeguarding obligation begins and ends in terms of the firm's business model and products. The FCA has clarified that the safeguarding obligation begins when the firm becomes

entitled to the funds, including instances where funds are credited to an account in the firm's name before segregation. Firms must ensure operational practices align with this requirement and document entitlement points clearly within the funds flow. Firms must clearly document their interpretation of when "redemption" occurs, ensuring this aligns with actual operational practice and current CASS 15 requirements. This should include clarification of whether redemption occurs:

- when the bank debits funds from the safeguarding account;
- when the bank accepts the payment instruction;
- when the firm's internal ledger is debited; or
- at another defined operational trigger point.
- Firms must assess and document the risks associated with timing differences (for example where an instruction is accepted but not executed), and ensure the defined redemption point matches the practical flow of funds within the firm.
- Best practice is to document this in the form of detailed funds flow diagrams depicting:
- the start and end of safeguarding;
- any period during which funds may not be safeguarded;
- associated operational and settlement risks

c) Ensure the customer terms and conditions mirror the funds flow requirements. Any changes in the funds flow should result in changes to the client terms and conditions and any supporting customer collateral;
d) put in place policies, processes and procedures to adequately safeguard relevant funds received from, or for the benefit of, payment services users;
e) documented rationale for all material decisions the firm makes in relation to the safeguarding process and the systems and controls they have in place; and
f) For AEMI's, have a clear understanding of when they are providing payment services unrelated to the issuance of e-money.
g) Clearly identify circumstances where funds may not constitute relevant funds and document treatment of such funds.

	Good practice	Poor practice
1	Clearly articulated definition of what constitutes relevant funds in the Safeguarding Policy, in the specific context of the firm's business, including in-scope and out-of-scope business and products.	Lack of clarity as to what constitutes relevant funds and what does not and whether the firm is acting as agent or distributor for another service provider

2	Clear articulation in both the Safeguarding Policy and client documentation (Terms and Conditions – ToC) of when the safeguarding obligation is triggered in the context of the firm's business, and when it ceases.	Lack of clarity as to when the safeguarding requirement begins and ends
3	Clearly defined processes and procedures to adequately safeguard relevant funds received from, or for the benefit of, payment services users, including a control matrix designed to ensure compliance with each Safeguarding requirement.	Lack of clarity around safeguarding processes and procedures
4	Firms should highlight any areas where co-mingling on receipt of funds may arise, and how these are addressed. For example, a client sends funds for both payment remittance and forward margin.	
5	**AEMIs only** Ability to identify between the issuance of e-money and unrelated payment services.	**AEMIs only** Failure to identify when unrelated payment services are being carried out.

3. Safeguarding methods

Under the PSRs and EMRs, there are two ways in which a firm may safeguard relevant funds:

- the segregation method – where relevant funds are segregated from all other funds the firm holds and, if the funds are still held at the end of the business day following the day on which they were received, to deposit the funds in a separate account with an authorised credit institution (or the Bank of England) or invest them in FCA approved secure liquid assets placed in a separate account with an authorised custodian.

- the insurance or comparable guarantee method – where relevant funds are covered by an insurance policy with an authorised insurer, or a comparable guarantee given by an authorised insurer or an authorised credit institution.

As set out in the FCA Approach document, it is possible to use both methods at the same time. Where firms utilise both safeguarding methods simultaneously, they should clearly document how funds are allocated between the segregation and insurance methods and ensure reconciliation processes reflect this allocation. Firms should also document the governance, monitoring and reporting processes used to ensure that the combined safeguarding framework remains compliant with regulatory requirements.

3.1 Key risks

- Funds are not adequately segregated from the member firm's own funds leaving them open to claims from other creditors
- Insufficient cover is provided under the insurance or guarantee method
- Risks arising from group structures, intra-group transfers or complex payment service provider chains, which may increase operational complexity and make the identification of relevant funds more challenging.

3.2 Guidance

Where a firm is subject to both CASS 7 (Client Money) and CASS 15 (Safeguarding), it must ensure that client money and safeguarded funds are held in separate accounts and are subject to distinct reconciliation, calculation and reporting processes in accordance with the interaction provisions set out in CASS 10A. Firms should ensure that operational processes clearly distinguish between these regimes to avoid co-mingling or misclassification of funds. Firms should clearly document any operational or settlement accounts used prior to safeguarding, including scheme accounts, correspondent accounts or prefunding arrangements, and explain how funds are identified and captured within the safeguarding process.

If firms are undertaking a non standard method for internal reconciliations, firms may want to consider having this process reviewed by an auditor and notifying the FCA of the decision.

3.2.1 Segregation method

We expect all member firms to:

a) Before placing relevant funds with an authorised credit institution or investing in assets to be held with a custodian, ensure that the third party is appropriately authorised by FCA or another EEA competent authority;
b) Ensure that relevant funds are not placed with another API or AEMI for safeguarding;
c) Perform daily safeguarding reconciliations. The reconciliation process should be automated wherever possible to reduce operational risk and ensure real-time accuracy, in line with the expectations of PS25/12 and safeguarding audit standards.
d) Before placing relevant funds with an authorised credit institution or investing in assets to be held with a custodian, carry out an initial documented assessment of the third party, including capital position, credit rating, liquidity profile, reputational risk, country risk and operational resilience. Where the firm also uses the insurance or guarantee method, equivalent due diligence should be applied to insurers, guarantors and any underlying underwriters.

Registered address c/o Dentons, 1 Fleet Pl, London EC4M 7RA. Company No. 07917853

e) Consider legal requirements, market practice and diversification of risk and document the rationale behind decisions. Periodic reassessment must occur at least annually and immediately upon any material adverse change, including downgrade in credit rating, regulatory action, material litigation, liquidity stress indicators, or significant market events affecting the safeguarding counterparty;
f) Ensure that safeguarding accounts are clearly identified as such within the name of the account;
g) Ensure safeguarding accounts are not used to hold any other funds or assets;
h) Firms should ensure that relevant funds are segregated promptly upon receipt, taking into account operational cut-off times, payment channels and intraday processing arrangements.
i) Ensure that any investment of relevant funds in permitted secure liquid assets complies with the requirements set out in the FCA Approach Document and CASS 15, and that appropriate due diligence and risk assessment has been undertaken before such investments are made; and,
j) Ensure that where relevant funds are held on a Member firm's behalf by agents or distributors, the agent or distributor segregates the funds in accordance with requirements and that the firm retains appropriate oversight and monitoring of those arrangements..

	Good practice	**Poor practice**
1	The firm carries out documented due diligence on any third party used to ensure they are correctly authorised, with selection approved at Board or defined Senior Management level.	• Due diligence is not performed or is not adequately documented. • Relevant funds are safeguarded with other entities in a payment chain such as APIs or AEMIs rather than authorised credit institutions • No evidence of approval by Senior Management
2	The due diligence includes a written credit assessment of the third party's capital position and leverage ratio etc.	No consideration is given to the third party's credit rating.
3	The due diligence includes a documented consideration of the third party's risk profile and activities.	No consideration is given to the third party's risk profile or activities.
4	Firm's Safeguarding Policy gives consideration to risk diversification between third party's holding	Risk diversification is not considered or documented.

Registered address c/o Dentons, 1 Fleet Pl, London EC4M 7RA. Company No. 07917853

	relevant funds and limits established per third party or as a percentage of money held.	
5	Periodic reviews are carried out at a defined frequency (at least annually) to ensure that the third party continues to be appropriate to hold relevant funds or assets.	Once appointed, no further due diligence is carried out on a third party
6	The title of the account(s) should be named in a way that shows it is a safeguarding account (rather than an account used to hold money belonging to the firm).	The title of the account(s) only identifies the firm not the purpose of the account
7	An annual audit check of all existing Safeguarding accounts, against the firms Bank Acknowledgment letter. Firms should also consider whether a refresher letter should be sought periodically so that records remain accurate.	
8	The firm identifies and transfers non-relevant funds received from clients such as fees and profits out of the safeguarding account(s) as often as possible each day, in line with the Safeguarding Policy.	Excess funds are held overnight in the safeguarding account without good reason
9	The firm identifies and transfers relevant funds received from clients such as mixed remittances into the safeguarding account(s) as often as possible each day, in line with the Safeguarding Policy.	Relevant funds are co-mingled with the firm's own funds for long periods intraday or overnight.

10	Where possible, written confirmation obtained from third parties confirming the trust status of the safeguarding account(s) signed by an authorised signatory.	The firm does not notify and confirm the status of its safeguarding account(s) in writing with the third party.
11	Documented assessments are maintained to demonstrate that any safeguarded funds are invested in an FCA's approved list of investments.	Assets are purchased without checking or documenting that they meet FCA criteria to be approved as liquid and secure.
12	The firm has identified instances where agents or distributors hold relevant funds and the segregation approach is clearly documented in safeguarding policy and agreements.	The firm has not taken into consideration relevant funds held at agents or distributors and has not implemented any measures to ensure that they are segregated on receipt.

3.2.2 Insurance or guarantee method

We expect all member firms to:

a) Ensure that the third party is appropriately authorised by FCA or another EEA competent authority
b) Where safeguarding arrangements involve investment in permitted secure liquid assets (such as money market funds) or reliance on the insurance or guarantee safeguarding method, firms should ensure that appropriate due diligence is undertaken and that the structure is supported by appropriate legal or regulatory analysis. Firms should ensure that any such arrangements align with applicable FCA guidance and, where appropriate, rely on recognised or FCA-accepted legal opinions regarding the safeguarding structure.
c) prior to taking out insurance or entering into a guarantee;
d) Notify FCA when changing the methods used for safeguarding. Firms must notify the FCA in accordance with the applicable regulatory notification requirements prior to implementing a change in safeguarding method. A change in safeguarding method is subject to regulatory notification rather than prior approval. While a firm may choose, as a matter of prudence, to engage with the FCA before implementing safeguarding insurance, responsibility for ensuring full compliance with CASS 15 rests with the firm and implementation should not be contingent on receiving formal confirmation from the FCA unless specifically requested by the regulator.

e) Before insuring with or taking a guarantee from a third party, carry out an initial documented assessment of the third party (underlying insurance provider), including the capital, credit rating, and risk profile of the third party, reputational risk and periodic assessments thereafter. This is akin to the banking DD that Firms should do if they adding insurance as an additional control to comply with the safeguarding rules;
f) Consider Legal requirements, market practice and diversification of risk should be considered and the rationale behind decisions documented;
g) Ensure that the insurance policy or guarantee meets the requirements of the PSRs and EMRs, covering all relevant funds held at any point, or a defined amount with any remaining relevant funds covered using the segregation method in section 3A above;
h) Ensure that a guarantee obliges the guarantor to assume primary liability to cover any relevant funds in an insolvency event;
i) Have controls in place to understand and appropriately manage liquidity;
j) Ensure that, in an insolvency, the proceeds from any insurance policy or guarantee will be paid into a Safeguarding account and be protected from other creditors. On annual renewal a Firm should validate that the bank accounts to where the insurance proceeds should be paid, if required, remain correct and valid. These accounts should be clearly identified as client accounts within their account title;
k) Ensure that where an AEMI carries out unrelated payment services, the insurance policy or guarantee covers both sets of services and be paid into separate Safeguarding accounts;
l) Make it clear in any Client Communications related to insurance that the insurance is not a surety for protection of client monies;
m) Retain on file, the "no claims declaration" which makes clear that the insurance proceeds are held on trust and not for the benefit of the Firm; and,
n) Ensure that relevant fund calculations are performed and retained and that the value of the insurance or guarantee is sufficient to cover requirements. In addition records should be held to demonstrate compliance with any requirements put in place by the insurer or guarantor (such as restrictions on the use of funds freed up through the use of the alternative method). The insurance policy, guarantee documentation, contact details of the insurer/guarantor, and the documented claims process (including trigger events and notification requirements) should be incorporated into the firm's CRP to ensure accessibility in a stress or wind-down scenario.

	Good practice	**Poor practice**
1	Firm's Safeguarding Policy gives consideration to risk diversification between third party's offering insurance or guarantees with limits established per third party or as a percentage of money held. The Safeguarding	Risk diversification is not considered or documented.

	Policy should also clearly document the manner in which insurance policy should be used and how daily requirement is adequately captured.	
2	The firm carries out documented due diligence on any third party to ensure they are correctly authorised, with selection approved at Board or defined Senior Management level.	• Due diligence is not performed or is not adequately documented. • No evidence of approval by Senior Management
3	The due diligence includes a written credit assessment of the third party's capital position.	No consideration is given to the third party's credit rating.
4	The due diligence includes a documented consideration of the third party's risk profile and activities	No consideration is given to the third party's risk profile or activities.
5	Periodic reviews are carried out at a defined frequency (at least annually) to ensure that the third party continues to be appropriate to offer insurance or guarantees.	Once appointed, no further due diligence is carried out on a third party
6	The firm should establish a Safeguarding account for the purpose of holding funds received pursuant to an insurance policy or guarantee in the event of an insolvency or for "top up" safeguarding of relevant funds in line with the Safeguarding Policy.	• No specific Safeguarding account is established • The account is used to hold other funds of the firm
7	The title of the account(s) should be named in a way that shows it is a safeguarding account (rather than an account used to hold money belonging to the firm).	The title of the account(s) only identifies the firm not the purpose of the account.

8	Segregation letters are obtained from third parties confirming the trust status of the Safeguarding account(s) signed by an authorised signatory.	The firm does not notify and confirm the status of its Safeguarding account(s) in writing with the third party.
9	The insurance policy should be periodically reviewed.	Claim cannot be processed due to changes in circumstances that are not reflected in the insurance policy.
10	Any guarantee issued accepts primary liability for the issuer in the event of an insolvency of the firm. There should be clear documentation on who the issuer is and periodic due diligence should be performed on the issuer.	Guarantees only provide secondary liability in the case that the institution fails to pay a debt or obligation

4. Records and Reconciliations

Firms should clearly document the data sources used in safeguarding calculations and reconciliations, including core payment systems, ledgers and any third-party systems used in the process.

Firms should implement internal controls designed to ensure the accuracy, completeness and integrity of source data, including validation checks, reconciliations and independent review by second-line risk or compliance functions.

As safeguarding reporting increasingly forms part of statutory audit processes, firms should ensure that calculation methodologies, data transformations, data lineage and reconciliation logic are fully documented and capable of independent verification.

Member firms must maintain accurate records of safeguarding arrangements under the PSRs and EMRs. These records should include:

- relevant funds segregated;
- relevant funds placed in an account with an authorised credit institution; and
- assets placed in a custody account.

In addition, member firms must keep accurate records that enable it to distinguish relevant funds and assets held:

- for an e-money holder/payment service user from any other e-money holder/payment service user; and
- for an e-money holder/payment service user from its own money.

The records should be sufficient to show and explain the member firm's transactions concerning relevant funds and assets.

To ensure the accuracy of these records, member firms should regularly carry out reconciliations between its internal accounts and records and those of any third parties safeguarding relevant funds or assets. Firms should ensure that safeguarding calculations capture all relevant funds received through operational channels prior to segregation, including funds received through payment schemes, correspondent banking arrangements or intermediary accounts.

Locations of safeguarding records should be clearly identifiable and logged within the safeguarding policy, the CASS resolution pack or within the wind-down plan of the Firm.

Firms must maintain a separate internal ledger of relevant funds to enable reconciliation against third party safeguarding accounts. While internal records may source data from external systems, firms must document the rationale for this approach and ensure that external data is transposed into the firm's own books and records.

Firms should also document within their Enterprise-Wide Risk Assessment (EWRA) the safeguarding impact and contingency measures should external data feeds or third-party systems become unavailable due to operational disruption.

Where a firm is subject to both CASS 7 and CASS 15, reconciliations, calculations and record-keeping processes must be performed separately for each regime to ensure no operational pooling or offsetting occurs between client money and safeguarded funds.

4.1 Key risks

- Inadequate records may make it difficult or impossible to identify for whose benefit relevant funds are being held
- Failure to reconcile regularly may conceal errors or shortfalls in safeguarding of relevant funds

4.2 Guidance

We expect all member firms to:

a) Maintain detailed and accurate records in respect of amounts held for e-money holders and payment service users;

b) Maintain detailed and accurate records in respect of relevant funds at client level and ensure reconciliations are capable of being converted into a single base currency value. Where funds are held in multiple currencies, clearly document the foreign exchange rate source used for currency conversion, the timing of rate capture and the rationale for the chosen methodology. Firms should ensure this methodology is consistently applied and aligned with applicable regulatory expectations:
   - the FX rate source used;
   - timing of rate application;
   - how volatility risk is managed;
   - how this aligns with applicable CASS requirements;
   - and how currency risk is mitigated within the control framework.

c) Maintain detailed and accurate records in respect of its own funds;

d) Ensure that relevant funds are not co-mingled with own funds inadvertently;

e) Firms must define and document the daily "reconciliation point" (cut-off time), explain why that point is operationally appropriate, and document any timing differences between internal and external systems. Where reconciliations are automated or dependent on external vendors, operational resilience documentation must include assessment of the safeguarding impact of system failure. Firms should also consider whether safeguarding balances held in multiple currencies create FX exposure or mismatches, and ensure this risk is appropriately managed within the safeguarding control framework.

f) Carry out reconciliations at least once per business day (excluding weekends and public holidays), and more frequently where required based on the size, complexity and risk profile of the firm.; and,

g) Correct any discrepancies promptly by paying in any shortfall or withdrawing any excess from safeguarding accounts. Reconciliation methodology should:
   - exclude artificial negative balances where this could mask shortfalls;
   - include unallocated funds;
   - include seized or frozen funds where relevant;
   - clearly document treatment of suspense and control accounts.

Where the treatment of particular balances (for example frozen funds, seized funds or disputed balances) requires interpretation of legal obligations, firms may need to obtain appropriate legal advice to determine the correct safeguarding treatment. Firms should ensure that their reconciliation methodology clearly distinguishes between the safeguarding requirement (the total amount of relevant funds that should be safeguarded) and the safeguarding resource (the total amount actually held in safeguarding accounts or covered by insurance/guarantee).

h) Where a firm maintains both a segregated safeguarding account and a separate relevant funds account, reconciliations should:
   a. Compare total safeguarding requirement against total safeguarding resource;and,
   b. Compare total safeguarding resource against funds physically held in safeguarding accounts on a T+1 basis.

c. include aged balances, including suspense items, unallocated funds or other balances pending investigation.

i) Ensure that relevant funds are segregated promptly upon receipt in accordance with regulatory requirements. Firms should document how intraday receipts, late cut-off payments and returned or failed transactions are treated to ensure no unintended delay in segregation occurs

j) Firms should document the rationale supporting their safeguarding calculation methodology, including assumptions, system logic and reconciliation processes. This documentation should be available for review by internal audit, external auditors and regulators

	Good practice	**Poor practice**
1	Firm's Safeguarding Policy should clearly set out the adequate procedures for reconciliation including the methodology and basis of reconciliation frequency.	Reconciliation is performed inconsistently
2	Where a firm maintains payment accounts or e-wallets for clients, these are clearly identifiable in the firm's systems.	Lack of distinction between payment service users' entitlements
3	Firm's maintain up-to-date internal ledger accounts for all third parties holding funds.	Firms rely on the third parties to provide account information
4	Firms own accounts are easily identifiable from Safeguarding accounts.	Lack of distinction between firm accounts and those used to hold relevant funds
5	Firms should list the bank accounts, per territory, and the type of account (ie segregated, safeguarding, business) so that they are clearly identifiable. The authorised signatories of the accounts should also be listed.	

6	Regular reconciliations carried out between the firms records of relevant funds held for payment services users, and the firm's internal ledger accounts for third parties holding those funds (internal reconciliation).	Reconciliations only carried out between client accounts and third party records
7	Regular reconciliations carried out between the firm's internal ledger accounts for third parties holding those funds and statements provided by those third parties (external reconciliation).	Reconciliations only carried out between client accounts and third-party records
8	Reconciliation of other accounts such as suspense accounts should be carried out on a regular basis to identify if there are any relevant funds that should have been identified and safeguarded. This should include AML/sanctioned frozen account and unallocated funds if they are deemed to be relevant.	Suspense accounts and other assets/liabilities not reconciled regularly
9	Reconciliations carried out at least daily or more frequently as required as per Safeguarding Policy, with reconciling items promptly identified and investigated.	• Sporadic or infrequent reconciliations • Reconciling items carried forward without adequate identification and investigation
10	Where resources permit, reconciliations are signed off by a senior member of staff who did not perform the reconciliation.	• Reconciliations performed and reviewed by the same person • No evidence of approval
11	Any excess or shortfall identified is moved out of or into the Safeguarding account(s) promptly in accordance with the Safeguarding Policy.	• Excess funds are maintained in the Safeguarding accounts without documented rationale • Shortfalls are not covered promptly from firm's own funds

5. Hybrid firms and independent FX services

The FCA Approach document allows firms that undertake activities unrelated to payment services to treat these outside of the safeguarding and other requirements of the PSRs and EMRs. In particular, paragraphs 10.18 and 10.20 refer to foreign exchange transactions carried out independently from payment services and carve these out from the safeguarding requirements.

FCA's view is that, in making a payment of currency to its customer in settlement of a foreign exchange transaction, an FX provider will be acting as principal in purchasing the other currency from its customer, and this does not constitute a payment service.

The extent to which a Member firm carries out foreign exchange transactions independently from its payment services will depend on its business model and contractual documentation, however it is important that this is clear to both customers and regulators alike.

5.1 Key risks

- Failure to identify whether foreign exchange transactions are carried out independently from payment services may result in incorrect identification and safeguarding of relevant funds, thereby corrupting the asset pool
- Customers may believe their funds are being safeguarded when they are not.

5.2 Guidance

We expect all member firms to:

a) Identify when they may be carrying out activities unrelated to payment services, including independent foreign exchange transactions;
b) Ensure that funds received for such unrelated services or independent foreign exchange transactions are not treated as relevant funds, or co-mingled with relevant funds inadvertently;
c) Ensure that all contractual and other customer documentation is clear as to when a transaction is subject to the PSRs/EMRs and when it is not;
d) Ensure that websites and marketing materials do not give the impression that funds received in settlement for unrelated services or independent foreign exchange transactions will be safeguarded when they are not;
e) Consider, when documenting the funds flow, how funds are treated where an FX transaction is linked to a payment instruction. Firms must:

- clearly document how safeguarding applies during the FX settlement process;
- distinguish between first-party FX and third-party payment flows;
- document the rationale for safeguarding treatment;

- ensure transparency to the customer regarding any period during which funds are not safeguarded;
- when FX settlement results in periods during which customer funds are not safeguarded, firms must clearly disclose this to customers and obtain explicit consent. The documentation should distinguish between first-party FX settlement flows and payment services, ensuring customers understand any temporary gap in safeguarding;
- obtain clear customer consent where funds are not subject to safeguarding during FX settlement.
- ensure that safeguarding treatment reflects the true economic substance of the transaction rather than solely the contractual structure.

f) Ensure the firm's financial promotions and onboarding disclosures are consistent with its documented safeguarding treatment of FX transactions and have been reviewed by Compliance following any safeguarding model change.

g) Where a firm makes material changes to its safeguarding model, including changes to its safeguarding method, reconciliation methodology or funds flow architecture, the firm should consider whether an interim independent review or audit is appropriate to provide assurance that safeguarding arrangements remain compliant.

	Good practice	**Poor practice**
1	Firm's Safeguarding Policy clearly articulates whether they are carrying out foreign exchange transactions independently from their payment services.	Little or no consideration has been given to whether unrelated activities or services are provided
2	Firms clearly identify in their processes how to treat funds received for unrelated activities or services.	Funds received for unrelated activities or services are co-mingled with relevant funds
3	Firms clearly identify in their client ToB when services are subject to the Safeguarding and other provisions of the PSRs and EMRs, and when they are not. Firms should be clear when client monies are not covered by FSCS, even though they should be safeguarded. Firms should ensure that customers understand the distinction between safeguarding protections and deposit protection schemes such as the FSCS.	Lack of clarity in contractual documentation what provisions apply to activities or services carried out independently from payment services

4	Firms clearly identify as part of their onboarding process when services are not subject to the Safeguarding and other provisions of the PSRs and EMRs.	Firms imply that funds are safeguarded at all times when they are not

6. Customer Communication

Firms should consider safeguarding disclosures as part of their Consumer Duty monitoring framework and assess whether customer understanding of safeguarding protections and limitations is evidenced through testing, complaints analysis or customer feedback.

In relation to safeguarding, this means a Firm should make clear to consumers what protections are afforded to their funds, and also any times that the funds are not protected also.

Firms should also make clear that client funds are not protected under the financial compensation scheme (FSCS).

This obligation should be communicated both at onboarding any time during the transactional flow, if the product means that safeguarding protection status is changing.

6.1 Key Risks

Clients are unclear of the protection of their client funds, which in the event of a liquidation event could result in loss of client funds

6.2 Guidance

We expect all firms to:

a) Communicate to clients in client facing collateral what means they use to protect client funds, whether this is via the segregation route, insurance or any other means;
b) Communicate to clients any instances, where client funds may not be protected during the transactional flow;
c) Ensure the client terms and conditions are clear, use simple language and communicate the provisions of safeguarding as they are applied in a transactional manner; and,

d) Make clear that FSCS protection does not apply to clients of an API or EMI
e) Firms should ensure that customer terms and conditions accurately reflect the firm's safeguarding framework and funds flow, including the points at which safeguarding begins and ends.
f) Firms must evidence customer understanding of safeguarding protections through testing, monitoring, and feedback analysis, in line with Consumer Duty expectations for measuring and demonstrating customer comprehension.

	Good practice	Poor practice
1	Firm's website has a designated area to communicate the safeguarding controls a firm applies	Firm websites or emails are silent to do not outlined the Firms safeguarding controls
2	Firms ensure safeguarding process is clearly posted, prominent, and any gaps are clearly communicated whether on the website, FAQ's or email communication	Client communication is not clear as to when safeguarding commences, and when it ends, along with any gaps in safeguarding
3	Firm staff are clearly trained and able to communicate the Firms' safeguarding controls	Staff are unable to deal with safeguarding queries from clients due to poor training
4	Client emails, and website make clear that FSCS protection is not applicable to API's or EMI's	Firm is silent on whether FSCS is applicable or not
5	On request, Firms are able to provide a copy of the client safeguarding letter from the Bank confirming client funds are protected	

7. Notifications of Safeguarding Breaches to the FCA

Firms must maintain a central Safeguarding Breach Register, aligned with CASS breach recording principles, documenting:

- nature of breach;
- date identified;
- root cause analysis;
- remediation steps;

- decision rationale on whether FCA notification was made;
- where notification was not made, documented reasoning and approval.

Firms should ensure compliance with SUP 15 (Notifications to the FCA) in relation to safeguarding breaches and ensure internal policies align with SUP escalation requirements.

Firms are required under regulation 20 of the Electronic Money Regulations 2011 and regulation 23 of the Payment Services Regulations 2017 to notify the FCA without undue delay if they have failed, or are unable, to comply with the safeguarding requirements.

In addition, firms must ensure compliance with the notification requirements set out in SUP 15 of the FCA Handbook in relation to safeguarding breaches or material safeguarding concerns.
Auditors are subject to statutory reporting obligations and must notify the FCA if, in their capacity as auditor, they become aware of a breach of safeguarding requirements or of deficiencies in organisational arrangements relating to safeguarding. For electronic money institutions, this may relate to the issuing of e-money and/or the provision of payment services.

When assessing whether a safeguarding breach should be notified to the FCA, firms should consider not only the size or financial impact of the breach but also its nature and systemic implications, including whether the issue indicates broader control weaknesses.

7.1 Key Risks

- Failure to notify the FCA as soon as a breach occurs may result in causing harm to the firm's clients;
- Failure to notify the FCA in accordance with the PSRs, EMRs, CASS 15 and SUP 15 would be viewed unfavourably and could attract enforcement action, including financial penalties or variation of permissions; and,
- As seen with previous cases, the FCA regard safeguarding breaches as serious and a failure to be transparent, which is a clear breach of principle 11, would likely compound the issue in the eyes of the regulator and increase the risk of enforcement action and public censure.

7.2 Guidance:

We expect member firms to notify the FCA in the following circumstances:

a) When a firm is unable to keep records of relevant funds and safeguarding accounts accurate and up to date;
b) When an error results in a failure to safeguard the correct amount of relevant funds (including under and over segregation).;
c) If the firm is unable to resolve reconciliation discrepancies;

d) When a firm is unable to comply due to the decision by a safeguarding credit institution to close a safeguarding account; and
e) If the firm fails to carry out the reconciliation process as frequently as appropriate.;

The firm's Notification Policy should define internal threshold triggers used when determining whether FCA notification is required and should reference specific examples set out within CASS and the FCA Approach Document.

When notifying the FCA of a breach, firms should give consideration to Principle 11 under PRIN2.1.1 and fully clear and transparent of the breach and the plans the firm has in place to address this breach. Firms should not be reluctant to report safeguarding breaches where appropriate. Notifications should demonstrate that the firm has undertaken a thorough root cause analysis, implemented remediation actions and clearly documented the rationale for concluding that the issue has been resolved.

	Good practice	**Poor practice**
1	Firm's Safeguarding Policy should have a clear articulation of what constitutes a breach as well as when and how to notify the FCA.	Little or no consideration has been given to what is a breach under the safeguarding guidance, how soon a firm is required to notify the FCA and what channel to use when notifying the FCA.
2	Consider Principle 11 of the Principles for business adopting the view of being fully transparent and open with the regulator to include the full details of the breach and the firms proposals in addressing this breach.	Not engaging with the FCA in a timely manner and/or providing vague details of the breach with no plans on how the firm plans to address the breach
3	Firms should notify the FCA as soon as they become aware of a breach or has reasonable grounds to suggest a breach has occurred	Firms delay the notification of a breach or do not notify the FCA in a timely manner when they have reasonable grounds to suggest a breach in the hope that they may
4	In order to adhere to number 3 above, firms ensure the reconciliation process is carried out as frequently as possible in order to capture a breach as soon as possible. Governance arrangements must ensure consistency between internal breach reporting and auditor notifications.	Poor management oversight of reconciliations not being carried out timely and appropriately resulting in either a delay in notification to the FCA or non-detection of a breach

8. Acknowledgment by authorised credit institution or authorised custodian of the status of the relevant funds or assets in the safeguarding account

The FCA Approach Document and CASS 15 require firms to obtain written acknowledgment from safeguarding institutions confirming the status of funds held in safeguarding accounts and confirming that the institution has no right of set-off or other claim over those funds except as permitted under the applicable regulations.

Where a firm deviates from the FCA's template acknowledgment letter, it must clearly document the rationale for deviation, assess any gaps created, and demonstrate how risks are mitigated. Firms must assess whether any deviation from the FCA template acknowledgment letter is permissible under CASS 15 and must document how any residual legal risk is mitigated.

Acknowledgment letters should be reviewed and refreshed at least annually. Firms should also obtain confirmation of authority from the bank (e.g. certificate of authority or equivalent) confirming that the signatory has authority to bind the institution.

8.1 Key risks

- Failure to obtain acknowledgment from the authorised credit institution or authorised custodian of the status of the relevant funds held on behalf of firms; and,
- Firm not having appropriate controls in relation to opening and closing safeguarding bank accounts results in inaccurate acknowledgment letters.

8.2 Guidance

We expect all member firms to:

a) Identify their total population of safeguarding bank accounts and ensure that these bank accounts are included on a safeguarding acknowledgment letter;
b) Have robust bank account opening and closing controls in place which help ensure the accuracy of the acknowledgment letters; and,
c) Where a firm is not able to obtain a safeguarding acknowledgment letter, the firm should retain evidence of the firms attempts to obtain the letter and supporting evidence which demonstrates compliance.
d) Firms should maintain robust controls governing the opening, modification and closure of safeguarding bank accounts, including documented approval processes, verification of authorised signatories and periodic confirmation with safeguarding banks that signatory records remain accurate.
Acknowledgment letters from safeguarding institutions must be reviewed annually to ensure continued accuracy.

Registered address c/o Dentons, 1 Fleet Pl, London EC4M 7RA. Company No. 07917853

	Good practice	Poor practice
1	Firm's Safeguarding Policy clearly articulates how safeguarding bank accounts are opened and acknowledgment letters obtained.	Little or no consideration has been given to safeguarding bank account opening process or process of obtaining safeguarding bank account acknowledgment letters
2	Firms will not use a safeguarding bank account until they have received a signed safeguarding bank account acknowledgment letter.	Firms use the safeguarding bank account before a counter signed acknowledgment letter is received from the counterparty.
3	Firms perform a periodic check between acknowledgment letters and internal system list of all open safeguarding bank accounts.	Firms do not have a process in place to periodically review the accuracy of acknowledgment letters.

9. CASS Resolution Pack

Firms must maintain a CASS Resolution Pack (CRP) in accordance with CASS 15 requirements. The CRP should:

- contain key safeguarding documentation, including bank acknowledgment letters, insurance policies, guarantees and contact details;
- document claims procedures;
- list safeguarding accounts and signatories;
- include reconciliation methodology;
- identify responsible individuals and deputies;
- link to incident management and wind-down planning;
- be reviewed at least annually;
- be subject to documented testing to ensure accessibility and completeness;
- clearly assign ownership and access permissions.

The CRP is not formally within the scope of the annual safeguarding audit but is commonly reviewed by auditors as part of their wider assessment of safeguarding governance and controls. Firms may refer to the AFEP CASS RP Master Template where appropriate.

Good practice		Poor practice	
CRP maintained in a clearly identifiable electronic folder with controlled access and named owner	CRP incomplete, dispersed across systems or with no clear ownership	CRP incomplete, dispersed across systems or with no clear ownership	CRP incomplete, dispersed across systems or with no clear ownership
CRP tested periodically (e.g. walkthrough or mock insolvency scenario) to confirm accessibility and completeness	CRP not tested and gaps only identified during audit or regulatory visit	CRP not tested and gaps only identified during audit or regulatory visit	CRP not tested and gaps only identified during audit or regulatory visit
CRP reviewed at least annually and updated following material changes	CRP only updated reactively following audit findings	CRP only updated reactively following audit findings	CRP only updated reactively following audit findings

10. Monthly reporting - Reg data

Firms subject to monthly regulatory reporting must document:

- data sources used;
- logic applied to calculations;
- FX conversion methodology applied;
- responsibility for compilation and submission;
- daily safeguarding reconciliation results, confirmation of the safeguarding method used. The figures submitted should also align with the firm's safeguarding and reconciliation results
- review and approval process;
- timing differences affecting reported data;
- retention of raw data files capable of being reconciled back to submitted returns.

Firms should ensure the regulatory return can be independently recalculated from underlying source data and reconciled to internal books and records.

Firms should ensure that data submitted in regulatory returns (including CMAR safeguarding data) reconciles to the firm's internal safeguarding calculation and reconciliation outputs. Any differences should be documented, explained and approved prior to submission.

Firms should ensure that internal safeguarding reporting and external regulatory reporting are aligned, and that senior management receives management information consistent with the data submitted to regulators.

	Good practice	Poor practice
1	Regulatory returns independently reviewed and signed off by an appropriately senior individual prior to submission Regulatory returns prepared and submitted by a single individual without review	Regulatory returns prepared and submitted by a single individual without review
2	Clear documented reconciliation between CMAR safeguarding data and the firm's safeguarding calculation and reconciliations Inability to evidence how CMAR figures link to safeguarding calculations	Inability to evidence how CMAR figures link to safeguarding calculation
3	Formal governance oversight of recurring data issues or late submissions Repeated data errors with no root cause analysis	Repeated data errors with no root cause analysis Repeated data errors with no root cause analysis
4	Regulatory communications relating to safeguarding centrally logged and tracked to resolution FCA queries handled informally with no audit trail	FCA queries handled informally with no audit trail FCA queries handled informally with no audit trail