Q.3. Do you agree with the priority areas we have identified, and our long-term ambition in each of these? Are there any other priority areas you think are important?

Answer:

Priority areas and ambitions are agreed with. Additional considerations suggested are as follows:

A. Grievance Redressal Mechanism
The advent of tokenisation is poised to disrupt markets and provide compounded benefits of easy liquidity of assets caused due to unhindered accessibility to notarisation via DSDs. This will exponentially burgeon scale of market activity.

Easy accessibility shall lead to proportionate surge in consumer grievances. Need for effective grievance handling might be considered as a priority area.

B. Money laundering and the Programmable DSS/ RTGS/ CHAPS ecosystem
More regulation may be deployed to manage how genuine programmed recurring payment mandates shall be treated to avoid raising false positive suspicious alarms for placement/ integration/ layering attempts. Especially, given the focus on the inclusion of non-sterling central monies in the ecosystem, drawing a line between the two is crucial to avoid misuse of the ecosystem.

C. PII Data to be kept off the DLT chain
DLT chains are irreversible. Any PII data that gets recorded has no chance of purging in future. Therefore, PII data must not be made subject to a ledger from I cannot be erased. Given the thrust on the traceability of a real legally responsible person behind each transaction, off-chain databases be deployed bifurcated from the chain.

D. Saving of access keys
Users should not be allowed in any possibility to save/ duplicate/ store their keys anywhere in their device, including any social account, browser cache, email, etc. The moment this is done, the key transitions into behaving like a "something that you have" authentication factor, against the intended "something that you know" factor, making it vulnerable to theft.

E. Succession and Inheritance of SIC
Secure inheritance of tokenised assets and prevention of their misuse thereof must be considered.

Q.6. How should safeguarding requirements for SICs be designed to deliver adequate client asset protection, while remaining proportionate, technology-agnostic and supportive of market development? Please consider whether and where safeguarding requirements should differ by type of SIC, how clients' ownership rights can be protected in the absence of external parties, such as a registrar, CSD or digital securities depositary that ensures legal ownership of SICs is accurately recorded and updated, and how safeguarding frameworks should support fungibility, interoperability and clear accountability as tokenised issuance, trading and post-trade models evolve.

Answer:

Following considerations may be made –

1. Security cost of tokenisation should scale proportionate to the value of the underlying asset, and not operate as a gate on tokenisation itself. Low value assets stand to benefit most from the fractionalised issuance this paper itself envisages, and should not be denied tokenisation merely for want of proportionate security cost.

Example: A low value asset may be secured at a lighter tier rather than being denied tokenisation altogether.

2. Assets beyond a decided threshold values be tiered. High value assets may be provided with heightened security in tokenised form and vice versa.

3. Accessibility of SICs must mandatorily include a "something that you are" factor within a multi-factor arrangement, since "something that you have" and "something that you know" factors are singularly more prone to compromise. Being non-revocable once compromised, a biometric factor is best deployed as one leg of authentication, not the sole gate.
   Example: A multi-factor arrangement requiring a fingerprint/ iris scan alongside a possession or knowledge factor, so compromise of one factor alone cannot access the SIC.

4. Keys may be sharded and stored via a threshold signature scheme (TSS) / multi-party computation (MPC) custody architecture, such that no single custodian ever holds the complete key. The shares held by each party, and the quorum required to sign, may be periodically refreshed (proactive secret sharing), so that keys remain non-static and variable over the asset's lifetime. [This measure shall curb the scope for the risk of employee frauds at banks, since no single employee or server ever has access to a static, complete key.]

5. Sharding and storage of keys may be buried in layers of security and random ambiguity.
   Example: Under an MPC custody arrangement, each custodian holds only a share of a distributed computation, not the underlying key value itself. Signing is performed jointly across custodians without the full key ever being reconstructed at any single point, and the shares are rotated on a defined cycle so that a share compromised in one cycle is worthless in the next.

6. The identity and total count of custodian parties in the signing quorum shall remain undisclosed, and the threshold required to sign (eg, 5-of-9) may itself be varied over time. This keeps the specific combination of parties required to compromise the key, at any given point in time, commercially unviable to identify or attack.

7. Regular rotation of shares and the signing quorum (proactive secret sharing) may be layered atop the above, so that the window in which a compromised share remains useful to an attacker is kept as short as possible.

8. An SIC is only as secure as its key's integrity. Therefore, any consistent miscreant action in the DLT chain may be treated as a financial offence.

9. Usage of AI in the process of keys of SIC should be structurally banned, for:

    a. Outputs of a trained AI model are comparatively more reproducible/predictable than a properly seeded cryptographic random number generator, weakening the very randomness that key security depends on if any AI model is involved in generating or managing a key.
    b. Any third-party AI vendor retaining logs, prompts, or checkpoints involved in key generation or management creates a duplication and exfiltration risk that sits entirely outside the custodian's control.

10. Accounts with links to proceeds of frauds, insider trading, etc, may be banned from the ecosystem.

From: **Chakradhar Kale** chakradharkale100@icloud.com
Subject: Fwd: Response to Call for Input: The Future of Tokenisation
Date: 4 July 2026 at 2:38 AM
To: tokenisedsecurities@fca.org.uk

Dear Mr Thomson-Ryder,

Further to my submission sent earlier today, I would like to confirm that I consent to the publication of my name as a respondent to this Call for Input.

Kind regards,
Chakradhar Premraj Kale,
The Finvocates.

---------- Forwarded message ----------
From: chakradharkale100@icloud.com
Date: 4 Jul 2026 2:23 am
Subject: Response to Call for Input: The Future of Tokenisation
To: tokenisedsecurities@fca.org.uk
Cc:

> Dear Mr. Thomson-Ryder,
>
> Please find attached my response to the joint FCA/Bank of England Call for Input, "The Future of Tokenisation: A joint vision from the authorities for UK wholesale financial markets" (May 2026).
>
> The attached document covers Question 3 (priority areas) and Question 6 (SIC safeguarding requirements).
>
> - **Threshold signature scheme (TSS) / MPC custody architecture for SIC keys** — a concrete answer to Q6's ownership-protection question that avoids single-point-of-custodian-compromise, with proactive share rotation to limit exposure windows.
> - **Proportionate, not prohibitive, security tiering** — security cost scaled to asset value rather than a threshold that would gate low-value assets out of tokenisation altogether, consistent with the paper's own fractionalisation objective (para 2.3).
> - **Grievance redressal and AML false-positive risk in the programmable DSS/RTGS/CHAPS ecosystem** — flags a gap not addressed in the current paper: distinguishing genuine programmed recurring payments from suspicious layering activity as the ecosystem scales.
> -
>
> Kind regards,
> Chakradhar Premraj Kale,
> The Finvocates.

Dear Mr Thomson-Ryder,

Further to my submission sent earlier today, I would like to confirm that I consent to the publication of my name as a respondent to this Call for Input.

Kind regards,
Chakradhar Premraj Kale,
The Finvocates.

---------- Forwarded message ----------
From: chakradharkale100@icloud.com
Date: 4 Jul 2026 2:23 am
Subject: Response to Call for Input: The Future of Tokenisation
To: tokenisedsecurities@fca.org.uk
Cc:

> Dear Mr. Thomson-Ryder,

Please find attached my response to the joint FCA/Bank of England Call for Input, "The Future of Tokenisation: A joint vision from the authorities for UK wholesale financial markets" (May 2026).

The attached document covers Question 3 (priority areas) and Question 6 (SIC safeguarding requirements).

Threshold signature scheme (TSS) / MPC custody architecture for SIC keys — a concrete answer to Q6's ownership-protection question that avoids single-point-of-custodian-compromise, with proactive share rotation to limit exposure windows.
Proportionate, not prohibitive, security tiering — security cost scaled to asset value rather than a threshold that would gate low-value assets out of tokenisation altogether, consistent with the paper's own fractionalisation objective (para 2.3).
Grievance redressal and AML false-positive risk in the programmable DSS/RTGS/CHAPS ecosystem — flags a gap not addressed in the current paper: distinguishing genuine programmed recurring payments from suspicious layering activity as the ecosystem scales.

Kind regards,
Chakradhar Premraj Kale,
The Finvocates.