Guidelines on Handling Customers Who Lack Mental Capacity

Issued 01 March 2011
Revised 28 September 2023
Updated 01 August 2026

A. Purpose and Scope

1. These Guidelines are intended to:
   a. safeguard the interests of customers who may lack mental capacity to make banking decisions;
   b. provide guidance to frontline staff on:
      - identifying indicators that a customer may lack mental capacity or may be experiencing potential cognitive vulnerability;
      - supporting customers who may have difficulty understanding, making or communicating decisions in relation to financial transactions;
      - recognising contextual indicators of financial harm, such as financial abuse, undue influence, coercion or scams given heighten concerns about a customer's decision-making ability; and
      - applying proportionate safeguards to reduce the risk of financial harm while respecting customer autonomy.

2. These Guidelines will apply to all banking accounts held by individual customers regardless of age.

3. Loss of mental capacity may be caused by dementia, a stroke, an accident or other medical conditions. As such, a loss of mental capacity is not necessarily associated with old age, and younger individuals may also lack mental capacity.

4. These Guidelines should be read together with Section C, which explains how concerns about mental capacity interact with scams, fraud, coercion, undue influence and other financial harm risks.

B. Background

1. Based on the National Population and Talent Division (NPTD)'s annual publication, around 1 in 4 Singaporeans will be aged 65 and above in 2030, making Singapore one of the fastest-ageing populations in Asia.[1]

2. As more people are affected by dementia and other capacity-impairing conditions, legislation is needed to balance a person's right to make his or her own decisions with the need to protect the person when he or she lacks mental capacity to do so.

3. To address this, the Mental Capacity Act (MCA)[2] was passed in Parliament on 15 September 2008 and came into force in 2010.

4. The Office of the Public Guardian (OPG), a division of the Ministry of Social and Family Development, works to "safeguard the interests of persons without mental capacity and support proxy decision makers within the framework of the MCA".

5. The MCA allows a person to make a Lasting Power of Attorney (LPA) to appoint proxy decision maker(s) (i.e. called a Donee[3]) to act on behalf of an individual (i.e. called a Donor[4]) in the event that he loses mental capacity. Depending on the scope of authority granted, this may include decisions relating to the Donor's property and affairs, including banking accounts and other financial matters. Where an LPA only covers personal welfare, banks should note that such authority does not, by itself, authorise financial or banking decisions.

[1] https://www.population.gov.sg/files/Population_in_Brief_2025.pdf

[2] Mental Capacity Act 2008 (Cap. 177A). Code of Practice available at msf.gov.sg/docs/default-source/opg/code_of_practice_sep2023_final.pdf

[3] A Donee is a person appointed under an LPA to act on the Donor's behalf in matters of personal welfare and/or property and affairs, when the Donor lacks mental capacity.

[4] A Donor is the person who makes an LPA, appointing one or more Donees to make decisions on the Donor's behalf if the Donor later lacks mental capacity.

C. Relationship with Other Risk Guidance

1. These Guidelines apply where there are concerns about a customer's ability to make a banking decision.

2. Such concerns may arise together with signs that the customer could be exposed to financial abuse, undue influence, coercion, scams, fraud or other financial crime.

3. These signs do not, by themselves, mean that the customer lacks mental capacity. They may, however, justify further engagement, escalation or safeguards where they raise concerns about the customer's understanding, intent, independence or ability to make the relevant banking decision.

4. Where the concern is primarily about financial abuse, undue influence, coercion, scams, fraud or other financial crime, and not about the customer's decision-making ability, banks should follow the relevant ABS, industry or internal guidance.

5. Where both mental capacity concerns and financial abuse, undue influence, coercion, scams, fraud, or other financial crime risks are present, staff should escalate through the bank's relevant internal processes so that the concerns are assessed and managed in parallel.

D. Definition of Lack of Mental Capacity

1. Under Section 4(1) of the MCA, "a person lacks capacity in relation to a matter if at the material time he is unable to make a decision for himself in relation to the matter because of an impairment of, or a disturbance in the functioning of, the mind or brain".

2. Lack of mental capacity cannot be established merely by referencing:
   a. a person's age or appearance; or
   b. a condition of the person, or an aspect of his or her behaviour, which might lead others to make unjustified assumptions about his or her mental capacity. For example, a person who has had a stroke or is living with dementia may not necessarily lack mental capacity. For further examples, refer to the Code of Practice — Mental Capacity Act.[5]

3. A person is unable to make a decision for himself or herself if he or she is unable to:
   a. understand the information relevant to the decision;
   b. retain that information;
   c. use or weigh that information as part of the decision-making process; or
   d. communicate his or her decision (whether by talking, using sign language or any other means).

4. Mental incapacity can be permanent, temporary or fluctuating, and should be assessed in relation to a specific decision at a particular point in time.

5. Banks and frontline staff are not expected to make clinical diagnoses. Their role is to identify observable concerns, support the customer's decision-making where possible, and escalate cases where there are valid doubts about the customer's ability to make the relevant banking decision.

[5] msf.gov.sg/docs/default-source/opg/code_of_practice_sep2023_final.pdf

E. Operational Assessment Principles

1. Banks should apply these Guidelines on a risk-based and proportionate basis, taking into account the nature, value and urgency of the transaction, the customer's observed ability to understand the transaction, and any relevant contextual risk indicators.

2. Frontline staff should remain alert to situations where a customer may have difficulty making, understanding or communicating a banking decision. These concerns may arise independently or together with contextual indicators of financial harm.

3. In assessing such situations, banks should adopt a structured, non-clinical approach by applying the decision-making test set out in Section D.

4. No single observation or indicator should be treated as determinative. Staff should consider the customer's overall behaviour, responses and surrounding circumstances before deciding on the appropriate course of action.

5. The fact that a customer makes a decision that appears unwise, unusual or financially disadvantageous does not, by itself, mean that the customer lacks mental capacity.

6. Detailed operational guidance is set out in the Annex.

F. Contextual Indicators of Financial Harm

1. Frontline staff should be alert to contextual indicators of financial harm where these arise together with concerns about a customer's decision-making ability.

2. Such indicators may include:
   - anomalies in a bank account, including large cash withdrawals;
   - sudden changes in account activity or banking practice;
   - unexplained withdrawals from a savings account; and
   - changes in third-party involvement with the customer's banking.

3. Staff should consider these indicators in context, together with the customer's explanations, behaviour and surrounding circumstances.

4. Where such indicators are present, staff should consider whether they raise concerns about the customer's understanding, intent, independence or ability to make the relevant decision.

5. Where the concern is primarily about financial abuse, undue influence, coercion, scams, fraud, or other financial crime risks, staff should follow the applicable ABS, industry or internal escalation process as described in Section C.

G. Handling and Escalation

1. Frontline staff should seek to establish the reason for large transactions or unusual withdrawals.

2. Frontline staff should check authorisation and documentation before acting for the customer.

3. Where there are signs that a third party may be exerting undue influence, staff should seek to engage the customer privately, in a language the customer is familiar with, to ascertain the customer's real intentions.

4. Where appropriate, such engagement should be conducted by at least two bank staff to provide independent observations and support objectivity.

5. If staff identify valid doubts about the customer's mental capacity, having regard to the decision-making test in Section D, they should alert a supervisor and tactfully advise the customer to have his or her mental capacity formally assessed by an accredited general practitioner or a medical specialist in mental health.

6. Pending the outcome of the formal capacity assessment and/or the appointment of a Deputy by the Family Justice Courts, the bank may apply safeguarding measures on the customer's account, which may include freezing the account.

7. Essential payments required for the customer's well-being, such as medical, healthcare or basic household expenses, should not be unduly restricted where proportionate safeguarding measures are applied.

8. Banks should act only on instructions from a Donee or Deputy where the applicable legal authority has been verified and the scope of authority covers the relevant banking matter. For customers who have made an LPA, frontline staff should:
   - request the original copy of the LPA (or a certified true copy from the OPG);
   - verify that the LPA is valid and has not been revoked (for example, by checking via the OPG);
   - verify the powers given to the Donee(s), i.e. personal welfare and/or property and affairs; and
   - where more than one Donee is appointed, verify whether they are authorised to act jointly, or jointly and severally.

H. Policies, Procedures and Training

1. Operational Implementation

Banks should ensure that the operational approach set out in Sections E, F and G is supported by clear internal processes and escalation protocols, including:

- identification and escalation of cases involving potential cognitive vulnerability or lack of mental capacity;
- supervisory review frameworks for cases requiring further assessment; and
- application of proportionate safeguards, including transaction delay or account restriction, where appropriate.

Banks should also ensure that internal procedures clearly define roles and responsibilities across frontline, supervisory, and second-line functions.

2. Use of Operational Playbook

Banks should incorporate the Annex into their frontline operating procedures as the primary reference tool for customer interactions involving potential concerns on a customer's mental capacity. In particular, banks should ensure that frontline staff are equipped to:

- apply a structured approach to observing, validating, deciding and acting;
- assess customer understanding and intent in a consistent manner;
- identify contextual financial harm indicators where these arise together with potential cognitive vulnerability;
- escalate cases appropriately; and
- apply proportionate safeguards aligned with the Guidelines.

3. Referral and External Support

Banks should establish processes to facilitate referral to appropriate community support services, where relevant and with the customer's consent.

This may include:

- referral pathways to Community Mental Health Teams; and
- escalation to Dementia Go-To Points for customers requiring immediate assistance.

Banks should ensure that such referral processes are implemented in a manner that:

- supports customer well-being;
- respects customer autonomy;
- protects customer confidentiality; and
- remains clearly distinct from transaction decision-making processes.

4. Conduct and Communication Guidance

Frontline staff should conduct interactions in a manner that is respectful, patient and non-confrontational.

In particular, staff should:

- use clear and simple language;
- avoid statements that may be perceived as dismissive, alarmist or stigmatising;
- ensure that the customer understands the discussion;
- communicate in a language that the customer is comfortable with; and
- take reasonable steps to protect the customer's confidentiality.

Where appropriate, staff may frame conversations in a supportive manner, for example by explaining that additional review is undertaken to safeguard the customer's interests and financial well-being.

5. Training and Capability Building

Banks should provide appropriate training to frontline staff to support the effective implementation of these Guidelines.

Training programmes should cover:

- awareness of potential cognitive vulnerability and mental capacity concerns;
- application of the structured assessment approach;
- communication techniques for engaging vulnerable customers who may require support;
- identification of contextual financial harm indicators where these arise together with potential cognitive vulnerability;
- use of referral pathways and escalation processes; and
- reference to separate financial abuse, undue influence, coercion, scams, fraud, or

other financial crime procedures.

Banks may also consider incorporating scenario-based training to support consistent application across different customer interaction contexts.

6. Application Across Channels

Banks should consider how the principles and approaches set out in these Guidelines may be applied consistently across different customer interaction channels, including:

- face-to-face interactions;
- telephone and video engagements; and
- digital or remote banking platforms.

In digital or remote contexts, banks may consider the use of:

- transaction prompts and confirmations;
- alerts for unusual activity; and
- escalation to assisted channels where appropriate.

7. Continuous Review

Banks are encouraged to periodically review and refine their policies, procedures and training to ensure continued effectiveness, taking into account:

- evolving customer needs;
- emerging risks, including new financial harm indicators or typologies; and
- developments in industry practices and community support frameworks.

8. Additional resources

- Refer to https://abs.org.sg/consumer-banking/banking-a-longevity-society for FAQs - Understanding Banking Practices for Lasting Power of Attorney and Deputyship in Singapore

- Banks can contact the OPG to be briefed on the MCA and LPA or for any clarifications. Banks are encouraged to contact the OPG at their hotline 1800 226 6222 or enquiry@publicguardian.gov.sg.

- How to make an LPA: https://www.msf.gov.sg/what-we-do/opg/lasting-power-of-attorney/how-to-make-a-lasting-power-of-attorney

- How to use the LPA: https://www.msf.gov.sg/what-we-do/opg/lasting-power-of-attorney/using-a-lasting-power-of-attorney

- Link to medical report template for LPA Activation/ Deactivation:

https://www.msf.gov.sg/what-we-do/opg/resources/forms (under Other Useful Forms For LPA)

- List of revoked and suspended LPAs: https://www.msf.gov.sg/what-we-do/opg/resources/revoked-and-suspended-lpas

- Information pertaining to the application as a deputy to make decisions on behalf of a person who lacks mental capacity can be found at the Family Justice Courts website: https://www.judiciary.gov.sg/family/deputyship

- For referral pathways to Community Mental Health Teams, please use https://mindline.sg/mental-health-service-providers/start

- To locate the nearest Dementia Go-To Points, please use https://web.cara.sg/go-to-points#download

ANNEX: Operational Playbook for Frontline Assessment of Customer Decision-Making Capability

This Annex provides an operational scaffold for frontline staff when there are potential concerns about a customer's decision-making ability in relation to a banking transaction. It does not restate the standards and principles in Sections D and E, or the handling guidance in Sections F and G, but provides a four-step flow, example questions and a triage table to support consistent decision-making by frontline staff . Indicators of financial abuse, undue influence or scams are included only as contextual factors that may support further engagement, escalation or safeguarding when there are potential cognitive vulnerability or capacity concerns.

How to read this Annex. Each step refers back to the relevant main section rather than repeating its content. Banks may adapt this playbook to align with their internal procedures, systems and training frameworks.

Step 1: Spot (Identify potential concerns)

At the start of the interaction, staff should be alert to indicators of potential cognitive vulnerability, lack of mental capacity, or contextual financial harm indicators that may be relevant to the customer's decision-making ability.

Staff should consider the following observable indicators[6]:

S/N	Category	Signs exhibited by the customer
1	Current transaction related	Unable to recall or explain purpose of bank visit or other information required to facilitate his/her request
2		Difficulty finding the right word to use or difficulty in articulating request
3		Unable to provide coherent reason for his/her request, e.g. large cash withdrawal
4		Repeatedly changing requests
5		Difficulty understanding bank staff even after rephrasing or simplifying words
6	Based on customer's own recounts	Forget PIN or bank signature more often than normal
7		Unable to recall transactions performed during recent visits to the bank, and what they were for

[6] Provided for by the Agency for Integrated Care (AIC)

8	General	Repeats same question or statement multiple times
9		Unable to tell the correct time of the day, month or the year
10		Appears unsure, tentative, lost, nervous, hesitant, evidently slow

The presence of such signs should trigger further engagement where appropriate but does not by itself establish that the customer lacks mental capacity.

Where no concerns are observed, staff may proceed with the transaction as normal. Where concerns arise, further assessment should be undertaken (Go to Step 2)

Step 2: Validate (Check Understanding and Intent)

Where concerns are identified, staff should seek to clarify the customer's understanding, intent and independence through calm and neutral engagement in a language the customer is familiar with, including private engagement where appropriate (see Section G). Banks should ensure that staff are trained and equipped to conduct such engagement consistently and sensitively, in line with Section H.

Examples of open questions:

- What would you like to do today?
- Can you tell me the purpose of this transaction?
- Who will receive the funds, and how do you know them?
- How did you arrive at this decision?
- What do you expect to happen after this transaction is completed?

Indicators to weigh in the response:

- Can the customer explain the transaction clearly in their own words?
- Is the explanation logical and internally consistent?
- Does the customer appear to be acting independently, or directed by another party?
- Does the customer show awareness of the consequences of the transaction?

Pay particular attention where the customer cannot explain the rationale, gives inconsistent responses, or shows signs of urgency, pressure or external influence.

Step 3: Decide (Determine Appropriate Course of Action)

Staff should use the framework below as a practical triage aid, applying judgment based on the overall interaction.

Level	Indicators	Action
Green	The customer demonstrates clear, consistent understanding, understands the transaction and appears to be acting independently	Proceed with the transaction
Amber	There are some uncertainties or inconsistencies requiring clarification. Contextual financial harm indicators may be present but the customer may still be able to explain the transaction	Escalate to a supervisor or second-line support
Red	The customer is unable to explain the transaction, or there are significant concerns regarding coercion, undue influence or financial harm	Pause or delay the transaction and escalate immediately

Step 4: Act (Apply Safeguards and Support)

The specific handling and safeguarding actions available, including supervisory escalation, formal capacity assessment, account restrictions and essential payments are set out in Section G. The Annex highlights how those actions map to the triage level:

- **Green:** proceed with the transaction; document observations where appropriate.
- **Amber:** apply measures such as allowing additional time, re-explaining the transaction in simpler terms, conducting the discussion in a private setting, or escalating for second-line review (see Section G).
- **Red:** pause or delay the transaction, alert a supervisor, and apply safeguarding measures including, where appropriate, freezing the account pending capacity assessment or appointment of a Donee or Deputy (see Section G). Continue to release essential payments for the well-being of the customer.

Where an LPA is in place, follow the verification steps in Section G.

For concerns primarily involving financial abuse, undue influence, coercion, scams, fraud, or other financial crime, staff should refer to Section C and the bank's relevant escalation process.

Concluding Note. This Annex supports a consistent frontline approach across the industry. Banks remain responsible for implementing arrangements that comply with applicable laws, regulations and their own internal policies, and for ensuring that customer autonomy and proportionality are maintained throughout.