BANK ĊENTRALI TA' MALTA
EUROSISTEMA
CENTRAL BANK OF MALTA

23 June 2026

Notice on the Supervisory Expectations on Fraud Risk Mitigation in the Instant Payments Environment

Introduction

In the context of the entry into force of Regulation (EU) 2024/886 on instant credit transfers ("IPR"), the Central Bank of Malta (the Bank), in line with Article 34A(1) of the Central Bank of Malta, Cap 204 of the laws of Malta, considers it appropriate to frame eleven (11) supervisory expectations regarding the implementation of the relevant requirements. This notice laying down the supervisory expectations is aimed at all those payment service providers (PSPs) providing the service of instant payments, as established under the IPR.

Relevant Documents

The Bank has considered the Technical Note issued in January 2026 by the Office of the Arbiter for Financial Services which inter alia addresses the adjustment of spending limits in scam-related cases. The Bank fully shares the objective of strengthening fraud prevention and ensuring effective consumer protection in the context of instant payments.

The Bank also refers to the clarifications issued jointly with the Financial Intelligence Analysis Unit (the FIAU) in December 2025, which outline the application of AML/CFT obligations in the context of instant payments. The expectations contained in this notice should be read in conjunction with the December 2025 clarifications, as regards the application of a risk-based approach, the need for pre- and post-transaction monitoring, and the requirement to assess transactions on a case-by-case basis.

1. Adjustment of Spending Limits and Application of Delay Periods

Article 5a (6) of Regulation (EU) 260/2012 ("SEPA Regulation"), as inserted by the IPR, requires PSPs to enable payment service users (PSUs) to modify their instant credit transfer limits at any time and at their sole discretion. Any such modification should take effect immediately. Hence, this provision effectively grants PSUs full control over their transaction limits, allowing them to adjust these as they see fit, and obliging PSPs to honour such adjustments without limitations whatsoever.

Pjazza Kastilja
Valletta VLT 1060
MALTA

Telephone: (+356) 2550 0000
E-mail: info@centralbankmalta.org
Website: www.centralbankmalta.org

This obligation applies on a 24/7/365 basis and reflects the real-time nature of instant credit transfers.

Thus, PSPs should ensure that the functionality to adjust spending limits is available across all payment channels through which instant credit transfers may be initiated, including digital channels and in-branch services, without restricting limit adjustments to specific channels or to business hours. Furthermore, the right to adjust the spending limits across all payment channels should be available to all types of PSUs, including both retail and corporate clients. This approach ensures that the objective of continuous access to instant payment services under the IPR is respected.

a. Delay Window on the Adjustment of Spending Limits

In September 2025, the Bank published a notice on the Introduction of a Delay Period for Instant Credit Transfers by means of which, the Bank adopted a risk-based approach and introduced a delay period after spending limits are adjusted. By applying this approach, the Bank tolerates the implementation of a temporary delay of up to six (6) hours before a spending limit adjustment, done remotely, takes effect.

In this notice, "remote adjustments to spending limits" should be understood as adjustments initiated through non-face-to-face channels, such as mobile banking, internet banking or telephone banking, where impersonation and social engineering fraud risks may be heightened.

Requests made physically at a branch, where robust in-person identification is carried out, present a different risk profile and, in principle, should not be subject to a delay in the absence of identifiable red flags.

This temporary delay period is not a mandatory requirement, but if implemented, certain parameters apply:

- It is intended as a proportionate safeguard against fraud risks, particularly in remote environments;
- shall not exceed six (6) hours from the time the adjustment is confirmed by the PSU and acknowledged immediately by the PSP; and
- applies irrespective of whether the request is made during or outside business hours.

Risk-based application of the delay window:

While the IPR requires PSPs to ensure that spending limits are adjusted with immediate effect, the six (6)-hour delay mechanism approach shall only apply as a temporary and proportionate supervisory allowance. The delay period must not be used to revert to a business-hours approval model.

PSPs should ensure that the temporary delay mechanism is applied only when objective indicators or red flags justify such enhanced scrutiny. It shall not be intended to operate as a default or systematic delay for all spending limit adjustments, especially in the absence of identifiable risk factors.

b. Intervention Within the Delay Window

Where the assessment of a request gives rise to identifiable red flags, PSPs are expected to use the permitted delay period to carry out enhanced monitoring and provide targeted warnings or notifications to the PSU, and, where necessary, establish contact through appropriate channels. The delay period mechanism should not create an open-ended discretion by PSPs to refuse or indefinitely postpone limit adjustments.

Where, after appropriate intervention within the six (6)-hour window, the PSU does not withdraw or cancel the original request, the spending adjustment limit shall take effect immediately upon expiry of the six (6)-hour delay.

c. Service Around the Clock

The Bank would like to clarify that any delay period applied should be measured in real time and not restricted to business or working hours. Payment services, particularly instant payments, are now available on a continuous basis. PSUs may therefore initiate and receive payments at any time, including evenings, weekends and public holidays.

In this context, fraud risks are also continuous. Limiting controls or delay mechanisms to business or working hours would create gaps in protection and would not reflect how payment services are used today. Accordingly, requests made on a Friday evening must not be deferred such that they only become effective on the next working day, being a Monday.

PSPs are therefore expected to ensure that their fraud monitoring, controls and interventions operate on a 24/7/365 basis, in line with the availability of the services they provide.

d. Baseline Setting and Temporary Adjustments of Spending Limits

PSPs are expected to establish default spending limits that are aligned with the typical risk profile and spending behaviour of the relevant PSU segment (e.g. retail or corporate PSUs).

Any adjustments to spending limits requested by the PSU should be accommodated in line with the provisions of this notice, including the application of a risk-based approach and, where appropriate, a temporary delay period.

PSPs are encouraged to offer a PSU-selected, time-bound limit increase (for instance, for a single payment or for a duration selected by the PSU, such as up to twelve (12) hours), after which the limit automatically reverts to the previous level unless the PSU confirms in writing or electronically that the new limit is intended to remain in place.

By way of example, this could be implemented through a simple user interface option within the relevant payment channel, whereby a PSU is prompted to select the nature of the limit adjustment (e.g. a one-time increase for a specific transaction, a temporary increase for a defined period, or a permanent adjustment). Such options may be presented through tick-boxes or similar selection tools, allowing a PSU to clearly indicate their intention at the point of request. This supports a more risk-based and proportionate approach to limit management.

Changes in spending limits can result in the need to reassess the PSU's risk profile from an AML/CFT perspective. While some institutions have systems that allow for a dynamic risk score, institutions that do not deploy such systems should have procedures in place for the said change to be considered from a risk perspective and assess whether the current risk score for the PSU is still applicable or otherwise. Temporary increases may not represent a significant change in risk, though the repeated and frequent use of such a functionality should equally result in a reassessment of the PSU's risk profile. PSPs should consider how the said change in spending limits may impact the level of transaction monitoring and scrutiny necessary to be applied with respect to the PSU. Any adjustments to the level of monitoring and scrutiny should take place as soon as possible following such change, including, where appropriate, by linking the change in spending limits to particular transaction monitoring measures.

2. Registration of New Devices

The Bank considers the registration of a new device as a high-risk event from a fraud perspective, particularly in cases of account takeover. As required under Directive (EU) 2015/2366 on payment services in the internal market ("PSD2") as transposed under

Central Bank of Malta Directive No.1 on the Provision and Use of Payment Services ("CBM Directive No.1"), registration of a new device must be confirmed using strong customer authentication (SCA). However, despite the two-factor authentication, the Bank is aware of instances where the fraudster still manages to install the mobile application on their device with access to the payment accounts of the victim. Some PSPs have already taken several practices which go beyond the requirements of the PSD2 to mitigate this risk. Accordingly, the Bank encourages the application of several best practices, as described further below. These best practices are aimed at maintaining a balance between consumer protection and user experience.

In this notice, 'registration of a new device' shall mean:

- **the registration of a new mobile device as the official registered point of contact with the user; and**
- **the registration of the mobile banking application on a new device.**

a. Delay Window Upon the Registration of a New Device

As a best practice, PSPs are encouraged to:

- apply a temporary delay period of up to six (6) hours for the initiation of payment transactions following the registration of a new device; and
- ensure that an out-of-band notification is sent in writing to the PSU (e.g. via SMS and/or email) informing them that a new device has been registered.

Such notifications should clearly inform the PSU of the action taken and provide instructions on how to contact the PSP immediately if the registration was not authorised.

These measures aim to provide PSUs with a window to react in case of unauthorised access, while maintaining a largely automated process.

b. Authorisation Through an Existing Trusted Device

Where a PSP applies a temporary delay period following the registration of a new device or the registration of the mobile banking application on a new device, the PSP may consider allowing the delay period to be shortened or bypassed where the PSU explicitly confirms the registration through an existing trusted device already registered with the PSP.

Such confirmation should be obtained through a secure, out-of-band mechanism, such as a push notification sent to the existing trusted device, requiring the PSU to clearly

approve the registration of the new device or application. The notification should clearly identify the action being authorised and should warn the PSU not to approve the request if they did not initiate it.

This approach should only be applied where the PSP has no objective indicators suggesting that the existing trusted device may be compromised or that the PSU is being manipulated. Where red flags are present, including unusual login activity, recent changes to credentials, suspicious location or IP address, or indicators of social engineering, the PSP should continue to apply appropriate safeguards, including the temporary delay period and enhanced monitoring.

c. Management of Device Access

As part of their internal fraud prevention framework, PSPs are encouraged to implement appropriate controls to manage the risks associated with the use of mobile banking applications across multiple devices.

PSPs may consider limiting the simultaneous active use of mobile banking applications to one (1) device per user, or, where not feasible, implement alternative safeguards that provide an equivalent level of protection against unauthorised access and account takeover.

Such safeguards may include, for example, enhanced authentication requirements, device binding, transaction monitoring linked to device behaviour, or real-time alerts when access is enabled on an additional device.

PSPs should provide PSUs with the ability to take immediate protective actions through all remote channels, including the capability to block or deactivate a payment instrument and to remove or disable access of a registered device.

Such functionalities should be available on a 24/7/365 basis and be easily accessible through digital channels, enabling PSUs to react promptly in situations of suspected unauthorised access or fraud.

These measures should form part of a broader fraud prevention framework and should not be relied upon as a substitute for effective monitoring and control mechanisms required to be implemented by the PSP.

PSPs are reminded that the addition of a new device can also have implications from an AML/CFT risk perspective. Not only should their monitoring systems capture any activity carried out through any such additional device so that they have a holistic overview and appreciation of the PSU's transactional activity, but the addition of a new device may

also present a change in risk profile of the PSU with all that this will imply in terms of the risk assessment and monitoring of the PSU's activity and transactions which may need to be varied to take into account any possible change in risk.

3. Customer Interaction and Staff Preparedness

PSPs should ensure that staff who have direct contact with PSUs, whether in branches or through remote channels, are appropriately trained to recognise and respond to potential fraud scenarios.

PSPs should be able to identify common warning signs of fraud and assist PSUs who may be in a vulnerable situation, including where the PSU is being manipulated or pressured into initiating a payment.

Where relevant red flags are identified, PSPs should take reasonable steps to alert the PSU that the transaction may be fraudulent and provide clear guidance before the transaction is executed.

The Bank also notes that, where there are objectively justified grounds to suspect fraudulent activity, PSPs may consider exercising the rights available under paragraph 44(2) of CBM Directive No.1, including the blocking of a payment instrument, while respecting the principles of appropriateness and proportionality to the risk identified.

4. Transaction Monitoring in an Instant Payments Environment

Given the nature of instant credit transfers, PSPs are expected to ensure that transaction monitoring frameworks operate in real time and cover both pre-transaction and post-transaction stages.

Pre-transaction monitoring is essential to identify and intervene in potentially fraudulent transactions before execution. Post-transaction monitoring remains important to detect suspicious patterns and support timely remedial actions where needed.

Reliance solely on post-transaction controls would not be sufficient in an environment where funds can be transferred and withdrawn within seconds.

PSPs should therefore ensure that their systems, processes and controls are designed to operate continuously and effectively in a 24/7/365 instant payments environment.

PSPs are also expected to ensure that payment transactions, in particular instant credit transfers, are visible to the PSUs through digital channels (including mobile and internet banking) without undue delay. PSUs should be provided with timely and accurate

visibility of debits and credits to their accounts, enabling them to monitor account activity and react promptly in case of unauthorised or suspicious transactions.

Any delays in the presentation of transactions should be limited to what is strictly necessary from a technical or operational perspective and should not undermine the real-time nature of instant payment services.

This expectation is consistent with the above-mentioned joint AML/CFT clarifications issued by the Bank and the FIAU, which clarifies that pre-transaction monitoring cannot be excluded or replaced entirely by post-transaction monitoring, even in an instant payments environment, as this would undermine the ability of PSPs to detect and report suspicious transactions in line with their AML/CFT obligations.

5. High-Risk Indicators and Enhanced Monitoring

PSPs are obliged to identify and monitor specific events or behaviours which may indicate an increased risk of fraud. These indicators should be used as part of a broader risk assessment framework to determine whether additional controls, warnings or interventions are required.

In addition to any other relevant risk factor, the following are non-exhaustive examples of high-risk indicators:

- Registration of a new device, particularly where this is followed by immediate payment activity;
- Abnormal use of the access device or software;
- Payment to a new payee, especially where the first payment is initiated shortly after a new device registration;
- Access or transaction initiation from an unusual location or IP address, including from a different country than the PSU's normal usage pattern;
- Recent adjustment of spending limits, particularly if followed by high-value or unusual transactions;
- High-value transactions, especially where these deviate from the PSU's typical behaviour;
- Detection of remote access, screen sharing and similar high-risk tools during a session.

PSPs should not rely on any single indicator in isolation. Rather, these indicators should be assessed collectively to determine whether there are objectively justified grounds to suspect fraudulent activity.

In line with the joint AML/CFT clarifications issued by the Bank and the FIAU, PSPs are expected to apply a risk-based approach when identifying and assessing such indicators, focusing on transactions that present unusual characteristics or give rise to suspicion, rather than applying blanket controls to all transactions.

Where such grounds exist, PSPs may apply appropriate and proportionate measures, including enhanced authentication, targeted PSU warnings, or temporary delays. Any such measures should be based on a case-by-case assessment and supported by objectively justified risk factors.

6. Use of Automated Controls and PSU Interaction

The Bank recognises that payment services are increasingly delivered through digital and automated channels on a 24/7/365 basis. In this context, PSPs are encouraged to make use of technology-driven solutions to manage fraud risks in a way that minimises friction in the PSU journey.

As a general principle, PSPs should not rely on routine or systematic manual contact with PSUs (e.g. telephone calls) as a primary control mechanism, as such approaches may not be scalable or compatible with real-time payment services.

Instead, PSPs are expected to implement effective automated controls, including real-time fraud monitoring and targeted warnings to detect and mitigate fraud risks.

PSPs are also encouraged to implement real-time, out-of-band notifications to inform PSUs when payment transactions are initiated through remote channels. Such notifications (e.g. via SMS, email or push notification) should be designed to provide PSUs with timely visibility of account activity and to enable them to react promptly in case of unauthorised transactions, while avoiding excessive or repetitive alerts that may reduce their effectiveness. In line with a risk-based approach. PSPs may benefit from prioritising such notifications in higher-risk scenarios, including transactions involving high values, new payees, recent changes to spending limits or device registration. These notifications should complement, and not replace, existing fraud prevention and transaction monitoring controls.

The implementation of dynamic, risk-based warnings at the point of payment initiation is also encouraged, particularly where identified risk indicators are present. Such warnings should be clear, prominent and tailored to the specific risk scenario, with the

objective of ensuring that the PSU is adequately informed before proceeding with the transaction. These warnings should be designed to interrupt potentially fraudulent transactions without introducing unnecessary friction in low-risk scenarios.

That said, where strong indicators of potential fraud are present and automated measures are not sufficient, PSPs must retain the ability to intervene through appropriate and proportionate means.

7. Detection of Remote Access, Screen-Sharing and Similar High-Risk Tools

The Bank is also aware of fraud typologies where victims are induced to install malicious or remote access applications, screen-sharing or remote-control software, enabling fraudsters to view or control the PSU's device and initiate payments or other account actions under the PSU 's credentials.

PSPs are expected to assess the risk posed by such tools as part of their fraud prevention framework. Where technically feasible, mobile banking applications and other remote payment channels should include controls to detect indicators of remote access, screen sharing, screen recording, mirroring or similar functionality which may expose the PSU to account takeover or social engineering fraud.

Where such indicators are detected during a login session, payment initiation, device registration or other actions, PSPs should apply appropriate and proportionate measures. These may include preventing or suspending payment initiation, restricting access to sensitive functions, issuing a clear written warning to the PSU, or requiring the PSU to disable the relevant functionality before proceeding.

The Bank expects PSPs to ensure that such controls are designed in a proportionate and privacy-conscious manner. The purpose of these controls should be limited to detecting security-relevant indicators and preventing fraud and should not involve general monitoring of the PSU's device or unrelated activity.

These measures should complement existing controls, such as restrictions on screenshots within mobile banking applications, device binding, transaction monitoring and targeted PSU warnings.

8. Verification of Payee

PSPs are expected to ensure that the Verification of Payee (VoP) service is available on a continuous basis (24/7/365), in line with Article 5c of the IPR.

Given the importance of VoP as a fraud prevention tool, PSPs should ensure a high level of operational resilience, including the implementation of appropriate contingency or fallback arrangements to minimise service disruption.

Where the VoP service is unavailable, this should be treated as an exceptional situation and may, depending on the circumstances, indicate non-compliance with the IPR.

PSPs should not rely solely on informing the PSU of the unavailability of VoP to mitigate or exclude liability.

The unavailability of VoP represents an increased risk of fraud. However, this should not result in the systematic delay or blocking of payment transactions. Payments should continue to be processed in line with the requirements applicable to instant credit transfers, unless additional risk indicators are present.

Where other red flags or risk factors are identified, PSPs may apply appropriate and proportionate measures, including enhanced monitoring, targeted warnings, or temporary delays, based on a case-by-case assessment.

This approach is also consistent with the mentioned joint AML/CFT clarifications which emphasises that transactions should not be rejected or restricted on a blanket basis, but rather assessed individually, considering the specific risk factors present.

9. Fraud Information Sharing

Given the increasing scale and sophistication of fraud, the Bank considers that individual PSPs acting in isolation will not be sufficient to effectively mitigate fraud risks across the payments' ecosystem.

In this regard, PSPs are encouraged to collaborate and share relevant information that may assist in the detection and prevention of fraudulent activity, such as information on accounts or IBANs suspected of being used for fraud.

The Bank notes ongoing developments at European level aimed at facilitating structured fraud information sharing across PSPs, including work undertaken by the European Payments Council (EPC) on a Fraud Information Distribution Arrangement (FRIDA), as well as forthcoming requirements under the proposed Payment Services Regulation (PSR). These initiatives are expected to provide a harmonised framework for information sharing across the Union.

PSPs should ensure that they have in place the necessary operational, technical and legal capabilities to support timely information sharing and to enable participation in emerging European-level arrangements. Effective fraud prevention increasingly requires

coordinated action at market level while ensuring that such arrangements are designed in compliance with applicable data protection and confidentiality requirements, as may be in force from time to time.

10. PSU Awareness and Fraud Prevention Communication

The Bank considers PSU awareness to be a key component of an effective internal fraud prevention framework, particularly in the context of authorised push payment fraud, where PSUs may be manipulated into initiating transactions.

PSPs are expected to implement ongoing communication measures aimed at increasing PSU awareness of fraud risks and promoting safe payment behaviours. Such measures should include periodic communications providing clear and practical guidance on how to identify and avoid common fraud typologies, including social engineering and impersonation scams.

In addition, PSPs are expected to undertake targeted awareness campaigns, using appropriate channels such as digital platforms, social media, branch networks and, where relevant, traditional media. These campaigns should be designed to reach different PSU segments and should focus on high-risk scenarios and emerging fraud trends.

Communication should be clear, accessible and proportionate, avoiding overly technical language, and should aim to influence PSU behaviour in a meaningful way. PSPs are encouraged to align the timing and content of such communications with observed fraud patterns, seasonal trends or specific risk events.

These measures should complement, and not replace, the implementation of effective transaction monitoring, controls and PSU interaction mechanisms as outlined in this notice.

11. Liability Considerations in Authorised Fraud Scenarios

The Bank acknowledges the challenges associated with authorised push payment fraud, where transactions are initiated and authenticated by the PSU, often as a result of manipulation or social engineering.

The assessment of liability in such cases should be conducted on a case-by-case basis, considering all relevant facts and circumstances, in accordance with CBM Directive No. 1 and other applicable legislative frameworks.

That said, where a PSP can demonstrate that it has implemented and applied, in a consistent and effective manner, the measures and controls outlined in this notice,

including, where relevant, real-time monitoring, risk-based intervention, targeted warnings, and appropriate PSU engagement, this should be taken into account as a significant factor in the assessment of whether the PSP bears any liability for transactions authorised by the PSU under CBM Directive No. 1.

Conversely, where material deficiencies are identified in the PSP's fraud prevention framework or in the application of such measures, this may be considered in the assessment of the PSP's responsibilities in the context of the CBM Directive No. 1 and other applicable legislative frameworks. This may include, by way of an example, situations where the VoP service is unavailable and the PSP has not implemented appropriate safeguards or mitigating measures to address the increased fraud risk associated with such unavailability.

Concluding Remarks

The Bank expects PSPs to take a proactive and forward-looking approach to strengthening their internal fraud prevention frameworks, ensuring that controls, systems and processes are aligned with the evolving risk landscape and the real-time nature of instant payment services.

The expectations outlined in this notice are intended to support a consistent and proportionate behaviour across the market, balancing the need for strong consumer protection with the provision of efficient and user-friendly payment services. PSPs are encouraged to engage collectively at market level to explore common standards to fraud risk mitigation, where appropriate.

PSPs are expected to review their current practices considering this notice and to conduct a gap analysis identifying any differences between their existing systems, controls and processes and the expectations set out herein.

The outcome of this gap analysis, including a clear implementation plan with defined timelines for addressing any identified gaps, should be submitted to the Bank within two (2) months from the date of publication of this notice.

PSPs are further expected to provide the Bank with periodic progress updates on the implementation of the identified measures, every two (2) months, until full alignment is achieved and, in any case, by no later than 1 July 2027.

The Bank will continue to monitor developments in this area closely, including through ongoing supervisory engagement, and may refine or expand these expectations as

necessary in line with regulatory developments at European level and emerging fraud trends.

Pjazza Kastilja
Valletta VLT 1060
MALTA

Telephone: **(+356) 2550 0000**
E-mail: **info@centralbankmalta.org**
Website: **www.centralbankmalta.org**