Feedback statement on Payment Card Requirements

Summary of Key Feedback Received and Bank Negara Malaysia Responses

In 2024, Bank Negara Malaysia (the Bank) issued a consultation letter (CL) on the Proposed Enhanced Requirements for Payment Cards, covering expectations in seven (7) existing policy documents namely: Debit Card, Debit Card-i, Credit Card, Credit Card-i, Charge Card, Charge Card-i, and the Debit Cash Out Facility for industry feedback.

The Bank wishes to record its appreciation to all respondents for providing valuable insights and feedback which have in turn assisted the Bank in finalising the requirements which are now captured in three (3) policy documents namely *Debit Card and Debit Card-i*, *Credit Card and Credit Card-i*, and *Charge Card and Charge Card-i.*

This review is centred on strengthening security controls for payment cards in response to escalating fraud threat, while also taking into account the need to preserve financial inclusion. All other requirements in the existing policy documents remain unchanged but may be subject to enhancements in future as part of the Bank's on-going review of its policy requirements.

The three (3) policy documents issued today have incorporated feedback and proposals received during the consultation period, where appropriate.

Key comments received and the Bank's responses are set out in this document.

1. **Transitioning to a more secure form of authentication for payment card transactions**

Feedback received:

Most respondents acknowledged the need to migrate away from SMS one-time-password (OTP) for authentication of online or card-not-present (CNP) transactions due to its known vulnerabilities.

Nevertheless, some respondents highlighted that implementing a full migration away from SMS OTP may unintentionally lead to certain cardholders being financially excluded, particularly those without compatible mobile devices or internet banking accounts.

This issue is also pertinent for credit cards given that such requirement could impact supplementary credit cardholders, as they may not have a direct banking relationship with the issuing financial institution (FI).

The Bank's response:

The Bank recognises the continued value of SMS OTP authentication for CNP card transaction for cardholders without compatible mobile devices or internet banking accounts and supplementary credit cardholders. Nevertheless, SMS OTP are known to be more susceptible to phishing and fraud, hence FIs should continue to migrate away from SMS OTP to a more secure form of authentication.

In balancing between mitigating the risks of financial exclusion and fraud prevention, FIs, subject to their internal risk assessment, may allow affected debit and credit cardholders (including supplementary credit card holders) to continue using SMS OTP as an authentication method for CNP transactions of up to RM250. This flexibility will ensure affected cardholders can continue to participate in e-commerce transactions whilst mitigating potential risk.

Nevertheless, this flexibility does not apply to the provisioning of payment cards on mobile wallets (e.g., Apple Pay, Samsung Pay), given the rising global fraud risks associated with card provisioning.

2. Empowering cardholder to manage payment card security features

Feedback received:

Respondents expressed concerns on expanding the default blocking requirement on credit cards, noting that it may create unnecessary friction as the inherent feature of credit cards already protect cardholders from immediate financial loss. While respondents are generally supportive of the enhanced requirements on debit cards which is to block CNP or overseas transactions on debit cards if no such transactions were conducted within the last twelve (12) months, they suggested for the Bank to consider providing alternative channels for financial institutions to implement the requirement.

The Bank's response:

The Bank has taken note of the industry's view and agrees to the following-

(a) The implementation of default blocking of CNP transactions for credit card products shall be based on respective FIs' risk assessment; and

(b) In implementing default blocking on CNP or overseas transactions for debit card products if no such transactions were conducted within the last twelve (12) months, FIs may either apply the control at the institutional level as stated in paragraph 25.2 of the Debit Card and Debit Card-i Policy Document and paragraph 41.1 of the Credit Card and Credit Card-i Policy Document or to provide a self-service toggle in the banking app or website to enable cardholders to manage their debit card settings for CNP or overseas transactions independently.

Notwithstanding paragraph (b), the Bank recommends the industry to provide a self-service toggle across all its payment card products to empower cardholders to manage their CNP and overseas transactions efficiently. In this regard, as FIs work to meet the requirements for debit card products above, FIs should consider developing a similar self-service toggle for credit card and charge card products to further enhance overall users' experience. The industry should also work collaboratively to standardise the placement of the toggle, and terminology adopted to explain its use to promote consistent communication and uniform implementation across FIs.

FIs that have implemented the self-service toggle for their cardholders should complement these efforts with continuous education on the use of this feature as well as other key security controls such as the kill switch, transaction limit management, and dispute processes as part of efforts to strengthen customer vigilance to combat fraud.

3. **Strengthening fraud investigation process and responsibilities of FIs and cardholders**

Feedback received:

Most respondents indicated that the implementation of a joint liability framework in the payment card space poses significant operational challenges due to the involvement of multiple parties in a card transaction. They also cited that existing rules and processes covering dispute and arbitration mechanisms are already sufficiently robust to safeguard consumer protection.

The Bank's response:

The Bank takes note of the industry's feedback. Therefore, the Bank is putting greater focus on strengthening FIs' internal investigation process to ensure fairer and more transparent outcomes for fraud victims. This includes outlining clear expectations on FIs to conduct robust investigations, by first identifying and addressing their internal weaknesses before assessing customers' negligence. FIs are also expected to improve transparency of the investigation process by clearly communicating investigation outcomes and the rights of the cardholders, including their rights to provisional crediting if investigations take longer to resolve as well as available redress channels if cardholders remain aggrieved by the outcome of the investigation.

4. **Elevating the security controls of payment card through the implementation of preventive measures**

Feedback received:

Some respondents highlighted that introducing a cooling-off period for new payment card activation could heighten friction for cardholders who expect immediate access to their new cards, especially in emergencies or for time-sensitive transactions. Such requirements may be less critical especially where rigorous identity verification procedures are already in place, ensuring that cards are issued to the rightful owner, hence reducing the risk of fraudulent card activation.

The Bank's response:

The Bank acknowledges that controls are already in place during the delivery and activation process of debit card, credit card and charge card products. In view of these safeguards, new debit card, credit card and charge card product

activation will not be subject to a cooling-off period where these safeguards are already in place.

BANK NEGARA MALAYSIA
19 December 2025