BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Interoperable Credit Transfer Framework

Exposure Draft

Applicable to:
1. Licensed banks
2. Licensed Islamic banks
3. Development financial institutions
4. Approved issuers of designated payment instruments
5. Registered merchant acquirers
6. Approved operators of payment systems

Issued on: 7 December 2017 BNM/RH/ED 028-8

This exposure draft outlines the Bank's proposed requirements to enable the interoperability of credit transfer services and facilitate collaborative competition (co-opetition) between banks and non-bank electronic money (e-money) issuers through fair and open access to shared payment infrastructure.

This proposal seeks to foster an efficient, competitive and innovative payment landscape in Malaysia by expanding the network reach for the provision of credit transfer services whilst ensuring adequate safeguards are in place to promote the safety and integrity of credit transfer systems and protect the rights and interests of customers of credit transfer services.

The Bank invites written feedback on the proposals in this exposure draft, including alternative suggestions that the Bank could consider and areas to be clarified. The written feedback should be supported with clear rationale and accompanying evidence or illustrations as appropriate to facilitate an effective review on this exposure draft.

Electronic submission is encouraged. All comments or suggestions with regard to this Exposure Draft should reach the Bank by **8 January 2018** to the following mailing address:

Pengarah
Jabatan Dasar Sistem Pembayaran
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur;

or addressed to the following officers:
1. Mr. Yip Kah Kit – yip@bnm.gov.my or 03-26988044 (ext.7876)
2. Ms. Joyce Lau – joyce@bnm.gov.my or 03-26988044 (ext.7337)

TABLE OF CONTENTS

PART A OVERVIEW 1
1 Introduction 1
2 Applicability 2
3 Legal provisions 3
4 Effective date 3
5 Interpretation 3
6 Related legal instruments and policy documents 8

PART B POLICY REQUIREMENTS 9
7 Interoperable credit transfer services 9
8 Fair and open access to shared payment infrastructure 10
9 Innovation sandbox and open APIs 12
10 Proportionate risk management 13
11 Customer protection 14
12 Provisions applicable to approved e-money issuers 15

Appendix 17
Limits and requirements for customer due diligence (CDD) for e-money accounts 17

PART A OVERVIEW

Introduction

1.1 Credit transfer refers to a payment service which allows a payer to instruct the institution with which the payer's account is held to transfer funds to a beneficiary.[1] In Malaysia, credit transfer systems such as Interbank GIRO (IBG) and Instant Transfer are accessible to the current and savings account (CASA) holders via Internet banking, mobile banking and ATM channels. Out of 24 million adults[2] in Malaysia, it is estimated that about 92% or 22 million individuals have access to CASA, of which there are 11.7 million[3] active Internet banking accounts with at least one transaction per month.

1.2 With a high penetration of debit cards[4] and mobile phones[5] in Malaysia, each adult is likely to carry both a debit card and a mobile phone that can be leveraged upon to make payments as a substitute for cash and cheques. Over the past 12 months, credit transfer services are increasingly being offered not only by banks via mobile banking applications, but also by non-bank electronic money (e-money) issuers through person-to-person (P2P) fund transfer service under their respective mobile payment applications. Credit transfer services, particularly when offered through the use of mobile devices, have the potential to complement the debit card as a cost-effective and convenient means to displace the use of cash and cheques. In this regard, the growing penetration of smartphones[6] and the availability of various mobile payment solutions offered by banks and non-bank e-money issuers have the potential to accelerate the migration to electronic payments (e-payments) and advance financial inclusion by enabling every adult in Malaysia to make or receive payment via electronic means.

[1] European Central Bank's (ECB) Glossary of Terms Related to Payment, Clearing and Settlement Systems.
[2] Individuals aged 15 and above.
[3] As at end-October 2017.
[4] For a population of 32.1 million, there were 45.4 million debit cards as at end-October 2017.
[5] For a population of 32.1 million, there were 42.8 million mobile phone subscriptions as at end-March 2017.
[6] Smartphone penetration is estimated at 70% and expected to increase further based on a recent survey conducted in 2015 (MCMC's Internet Users Survey 2016).

1.3 Given the importance of network effects in promoting greater payment efficiency, banks and non-bank e-money issuers should collaborate at the infrastructure level by leveraging on shared payment infrastructure and ensuring the interoperability of their respective credit transfer services. This would bring about economies of scale and expand network reach, thus lowering costs while encouraging competition at the product and service level. This is envisaged to create a more efficient, competitive and innovative payment landscape that fosters continuous improvements in payment services to keep pace with emerging technological changes and changing user demands.

1.4 This Policy Document outlines requirements aimed at:

(a) enabling interoperability of credit transfer services leveraging on shared payment infrastructure to expand network reach and avoid market fragmentation;

(b) ensuring fair and open access to shared payment infrastructure to promote a level playing field and foster collaboration at the infrastructure level;

(c) ensuring effective oversight of shared payment infrastructure to minimize risk of disruption to credit transfer systems;

(d) encouraging innovation through the establishment of innovation sandbox facilities and publication of Application Programming Interfaces (APIs) by an operator of shared payment infrastructure;

(e) establishing risk management measures proportionate to the nature, scale and complexity of the activities and risk profile of the respective providers of credit transfer services; and

(f) strengthening customer protection and fostering confidence in the use of credit transfer services.

Applicability

2.1 This Policy Document is applicable to all licensed banks, licensed Islamic banks, prescribed development financial institutions, approved issuers of

designated payment instruments, registered merchant acquirers and an approved operator of a payment system that operates a shared payment infrastructure as defined in paragraph 5.2.

Legal provisions

3.1 The requirements in this Policy Document are specified pursuant to sections 18, 33, 47, 49 and 123 of the Financial Services Act 2013 (FSA), sections 43, 57 and 135 of the Islamic Financial Services Act 2013 (IFSA), sections 41 and 42C of the Development Financial Institutions Act 2002 (DFIA) and section 83 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA).

3.2 For the purpose of paragraph 3.1, the requirements in paragraphs 7.1, 7.3, 7.6, 8.6, 10.3, 10.4, 11.1 and 11.2 of this Policy Document seek to minimize the risk of disruption to credit transfer systems, and ensure that adequate safeguards are put in place by the financial institutions to promote the safety and integrity of credit transfer systems and protect the rights and interests of customers of credit transfer services.

Effective date

4.1 This Policy Document shall come into effect on **1 July 2018**.

Interpretation

5.1 The terms and expressions used in this policy document have the same meanings assigned to it in the FSA, IFSA, DFIA or AMLATFPUAA as the case may be unless otherwise defined in this policy document.

5.2 For the purpose of this policy document–

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"Application Programming Interface or API" means a set of commands, functions, protocols and objects used to create software and interact with external systems;

"approved issuer of e-money" means a person approved under section 11 of the FSA or IFSA to issue e-money and for the avoidance of doubt, this may include a banking institution or a non-bank issuer of e-money;

"approved operator of a payment system" means an operator of a payment system approved under section 11 of the FSA or section 11 of the IFSA;

"Bank" means Bank Negara Malaysia;

"bank account" means a current account, a savings account or an account where a line of credit is extended by a banking institution to a customer;

"**banking institution**" means a licensed bank as defined under the FSA, a licensed Islamic bank as defined under the IFSA or a development financial institution prescribed under the DFIA;

"**credit transfer**" means a payment service which allows a payer to instruct the institution with which the payer's bank account or e-money account is held to transfer funds to a beneficiary in another bank account or e-money account, irrespective of any underlying obligation between the payer and the beneficiary. For the avoidance of doubt, any reference to "credit transfer" in

this policy document shall include a reference to both a fund transfer transaction and a purchase transaction regardless of the technology used to facilitate the transaction including Quick Response (QR) code, and this shall include but not limited to a credit transfer transaction where a payment card is used to generate the information required to make or receive a credit transfer from a bank account or an e-money account;

"customer" means a financial consumer as defined under section 121 of the FSA and section 133 of the IFSA;

"customer data" means personal data as defined under the Personal Data Protection Act 2010 and credentials that are used for customer authentication and transaction authorisation, and such other customer data as may be specified by the Bank;

"electronic money" or "e-money" means a payment instrument or an Islamic payment instrument, whether tangible or intangible, that stores funds electronically in exchange for funds paid to the issuer and is able to be used as a means of making payment to any person other than the issuer;

"eligible credit transfer transaction" means a credit transfer transaction but excludes:

(a) bulk payment including Interbank GIRO (IBG) transactions;
(b) bill payment including JomPAY transactions;
(c) electronic or mobile commerce transactions including Financial Process Exchange (FPX) transactions; and
(d) such other types of credit transfer transactions as may be specified by the Bank;

"eligible issuer of e-money" means an approved issuer of e-money with substantial market presence based on such criteria as may be specified by the Bank;

"financial institution" means a banking institution, an approved issuer of a designated payment instrument and a registered merchant acquirer;

"innovation sandbox" means a contained non-live test environment that mimics the functionality of a production environment, established by an operator of a shared payment infrastructure in which participants and other third parties may test their product, service or solution[7];

"**inter-bank credit transfer**" means any credit transfer in Malaysia between a bank account maintained with a banking institution and another bank account maintained with another banking institution but excluding any fund transfer between bank accounts maintained with the same banking institution;

"**inter-scheme credit transfer**" means any credit transfer in Malaysia between–

(a) a bank account maintained with a banking institution and an e-money account maintained with an approved issuer of e-money; or

(b) an e-money account maintained with an approved issuer of e-money and another e-money account maintained with another approved issuer of e-money,

but excluding any fund transfer between e-money accounts maintained with the same approved e-money issuer;

"licensed bank" means a person licensed under the FSA to carry on banking business;

"licensed Islamic bank" means a person licensed under the IFSA to carry on Islamic banking business and includes a licensed international Islamic bank;

[7] For avoidance of doubt, this is separate and distinct from the 'fintech regulatory sandbox' established under the Financial Technology Regulatory Sandbox Framework issued by Bank Negara Malaysia, which is a live environment where approved applicants may test any financial product, service or solution subject to specified parameters and timeframes.

"**National Addressing Database**" means a central addressing repository established by an operator of a shared payment infrastructure that links a bank account or an e-money account to common identifiers of the account holders such as mobile phone number, National Registration Identity Card (NRIC number), company registration number or business registration number, and facilitates payment to be made to a recipient by referencing the recipient's common identifiers;

"operator of a shared payment infrastructure" means an approved operator of a payment system under the FSA or the IFSA, as the case may be, that operates a payment system that is established and located in Malaysia and facilitates inter-bank credit transfer and/or inter-scheme credit transfer;

"passcode" means a password or code that is used to authenticate the identity of a customer and to authorise a transaction. A passcode may consist of numbers, letters, a combination of both, or a phrase. Examples of a passcode include:

(a) password;
(b) one-time password (OTP);
(c) personal identification number (PIN); and
(d) code generated by a security device.

"payment card" means a debit card, debit card-i, credit card, credit card-i, charge card, or charge card-i as defined under the Financial Services (Designated Payment Instruments) Order 2013 [P.U.(A)202] and the Islamic Financial Services (Designated Payment Instruments) Order 2013 [P.U.(A)208];

"prescribed development financial institution" means a development financial institution prescribed under the DFIA;

"purchase transaction" means any transaction for the purchase of goods or

services;

"registered merchant acquirer" means an operator of a payment system that provides merchant acquiring services registered under section 17 of the FSA;

"security device" means a token or other device that generates a passcode;

"shared payment infrastructure" means a payment system that is established and located in Malaysia and facilitates inter-bank credit transfer and/or inter-scheme credit transfer; and

"sponsor bank" means a banking institution that provides a financial institution with access to a shared payment infrastructure via the banking institution for the purpose of enabling inter-bank credit transfer and/or inter-scheme credit transfer within Malaysia.

Related legal instruments and policy documents

6.1 This policy document must be read together with other relevant instruments and policy documents that have been issued by the Bank, including the following:

(a) Guideline on Electronic Money (E-Money);

(b) Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Institutions (Sector 1); and

(c) Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4).

6.2 In the event of any discrepancy between the provisions in this policy document and the policy documents listed in paragraph 6.1 above, the provisions in this policy document shall prevail and take precedence.

PART B POLICY REQUIREMENTS

Interoperable credit transfer services

S 7.1 A banking institution and an eligible issuer of e-money shall–

(a) enable its customers to register their account information and common identifiers in the National Addressing Database;

(b) ensure that its customers are able to make payment to and receive payment from another customer of the same or another banking institution or eligible issuer of e-money, including through the use of common identifiers registered in the National Addressing Database and via the interoperable QR code scheme established under paragraph 7.4; and

(c) waive the transaction fee imposed on its customers who are either the sender or the recipient for any eligible credit transfer transaction up to RM5,000 per transaction or such other amount as may be specified by the Bank.

G 7.2 Notwithstanding sub-paragraph 7.1(c), a banking institution and an eligible issuer of e-money may impose a fee on customers who are on-boarded as merchants, for value-added services provided in addition to the credit transfer services and the facilities specified in sub-paragraphs 11.1(a), (b) and (c), and subject always to compliance with sub-paragraph 11.1(d).

S 7.3 A financial institution shall ensure that any inter-bank credit transfer transactions and inter-scheme credit transfer transactions are processed in Malaysia via an operator of a shared payment infrastructure to facilitate the Bank's effective oversight on such operator.

S 7.4 An operator of a shared payment infrastructure shall establish an interoperable QR scheme and a common QR code that facilitate the customers of its participants to make inter-bank credit transfer and inter-scheme credit transfer transactions.

S 7.5 An operator of a shared payment infrastructure shall ensure that the common QR code established under paragraph 7.4 will enable a customer of its participants to receive payment from another customer of any of its participants.

S 7.6 A banking institution and an eligible issuer of e-money shall facilitate its customers to generate a common QR code established under paragraph 7.4.

S 7.7 An operator of a shared payment infrastructure shall develop technical standards and business rules to facilitate interoperability of credit transfer services.

S 7.8 The technical standards and business rules to be established by an operator of shared payment infrastructure under paragraph 7.7 shall include but not limited to secure QR code standards, API standards, communication protocols, and standard operating procedures for populating and operating the National Addressing Database.

Fair and open access to shared payment infrastructure

S 8.1 An operator of a shared payment infrastructure shall–

(a) allow a financial institution, which shall not be limited to a banking institution or an eligible issuer of e-money, to have access to the shared payment infrastructure which shall include the switching and clearing system and the National Addressing Database, based on the access requirements established in accordance with sub-paragraph (b) below;

(b) establish objective, non-discriminatory and risk-based access requirements to the shared payment infrastructure, including the requirements to be fulfilled by a sponsor bank, which shall not inhibit access except as reasonably necessary to safeguard against settlement, operational and business risks, and to protect the financial and operational stability of the payment system;

(c) publicly disclose the following information, minimally in its website:

(i) access requirements to the shared payment infrastructure;

(ii) name of its participants;

(iii) timeframe in which a decision will be made in relation to an application by a financial institution for access to the shared payment infrastructure; and

(iv) timeframe in which a decision will be made in relation to an appeal made by a financial institution under paragraph 8.3 below; and

(d) notify a financial institution in writing of its decision on whether to allow the financial institution to have access to the shared payment infrastructure and the relevant access conditions or reasons for refusal of access, where applicable.

S 8.2 An operator of a shared payment infrastructure shall establish an appeal handling process to hear an appeal made by a financial institution that has been denied access to the shared payment infrastructure or disagrees with the access conditions imposed by the operator.

S 8.3 The appeal handling process established under paragraph 8.2 above shall minimally include the following:

(a) a financial institution may submit its appeal to a Board committee of the operator which comprises at least three individuals (one of whom will be the chair), who are all independent directors;

(b) in determining an appeal, the Board committee shall have regard to the provisions set out in this policy document; and

(c) the Board committee shall notify the financial institution in writing of its decision in relation to the appeal of the operator's decision and the reason for any rejection of the appeal, where applicable.

S 8.4 Without prejudice to paragraph 8.1, an operator of a shared payment infrastructure shall–

(a) establish transparent, objective and non-discriminatory fee structure applicable to its participants;

(b) disclose to its participants the basis in which the fee structure is determined; and

(c) disclose to its participants the manner in which the fees collected from its participants are utilised.

S 8.5 An operator of a shared payment infrastructure shall establish rules for the withdrawal, suspension and termination of the access by a participant to the shared payment infrastructure, which shall–

(a) clearly define the circumstances that may give rise to such events; and

(b) set out the rights and obligations of participants during such events.

S 8.6 A sponsor bank shall–

(a) establish objective, non-discriminatory and risk-based requirements to be fulfilled by a sponsored financial institution for access to a shared payment infrastructure via the sponsor bank;

(b) publicly disclose the following information, minimally on its website:

(i) a description of the sponsor bank services offered; and

(ii) the requirements established under sub-paragraph (a).

Innovation sandbox and open APIs

G 9.1 An operator of a shared payment infrastructure should coordinate with its participants to–

(a) publish APIs;

(b) establish an innovation sandbox facility; and

(c) permit any third party to use the APIs published under sub-paragraph (a) and the innovation sandbox established under sub-paragraph (b), for the purpose of experimenting and testing of a new product, service or solution.

S 9.2 Where APIs are published under paragraph 9.1(a), an operator of a shared payment infrastructure shall define the process in relation to information handling, authentication and authorisation in a manner that is consistent with relevant laws, policies and guidelines dealing with data privacy and security.

Proportionate risk management

S 10.1 An operator of a shared payment infrastructure shall establish procedures, controls and measures for the management of risks associated with inter-bank credit transfers and inter-scheme credit transfers, including but not limited to credit or settlement risk, liquidity risk, security risk and risk associated with data privacy.

S 10.2 An operator of a shared payment infrastructure shall ensure that the procedures, controls and measures established under paragraph 10.1 are proportionate to the nature, scale and complexity of the respective activities and risk profiles of its participants.

S 10.3 In circumstances where the money laundering and terrorism financing (ML/TF) risks are assessed to be low and are within the limits set out in the **Appendix**, an approved issuer of e-money[8] may perform no customer due diligence (CDD) or may perform simplified CDD measures as stipulated in the **Appendix**, as the case may be.

S 10.4 For the purpose of paragraph 10.3, an approved issuer of e-money shall–

(a) ensure that it has put in place adequate internal controls to mitigate ML/TF risks;

(b) ensure that it has put in place appropriate systems and controls to ensure compliance with the relevant limits stipulated in the **Appendix** including a system to detect when a customer is approaching the limits and trigger specific CDD measures;

(c) conduct CDD on customers that are on-boarded as merchants for purchase transactions; and

(d) conduct enhanced CDD if–

(i) it has knowledge or suspicion of ML/TF;

(ii) it becomes aware of anything that raises doubt as to the identity or

[8] For the avoidance of doubt, an approved issuer of e-money refers to a banking institution or a non-bank entity that is approved to issue e-money under the FSA or the IFSA.

intentions of the customer or the beneficial owner; or

(iii) the business relationship with the customer or the beneficial owner is assessed to pose a higher ML/TF risk.

S 10.5 The Bank may require an approved issuer of e-money to observe a lower account limit and/or a lower transaction limit or to perform additional CDD measures other than that stipulated in the **Appendix** based on the assessment of the ML/TF risks and/or the adequacy of the internal controls of the approved issuer of e-money.

S 10.6 An operator of a shared payment infrastructure shall establish rules that shift the liability for fraud losses in relation to an inter-bank credit transfer transaction and/or an inter-scheme credit transfer transaction to its participant with the weaker security or AML/CFT controls.

S 10.7 An operator of a shared payment infrastructure shall establish a transparent and efficient dispute resolution mechanism to resolve dispute between its participants in relation to the services provided via the shared payment infrastructure.

Customer protection

S 11.1 A financial institution shall–

(a) provide a convenient means for its customers to manage their transaction limits of the credit transfer services offered, minimally via its website or mobile application;

(b) provide instant notification to its customers of any transaction;

(c) provide a convenient means for its customers to check their account balance on a real-time basis, minimally via its website or mobile application;

(d) disclose the pricing and information on the credit transfer services rendered to customers in a manner that is transparent and would facilitate comparison and informed decision-making by the customers;

(e) ensure customer data are securely protected and stored onshore including but not limited to deploying preventive and detective controls to prevent any occurrence of loss, theft or unauthorised access of customer data; and

(f) take reasonable steps to ensure its customers are adequately alerted and provided with updated safety tips that are practicable and effective, including but not limited to the obligations set out in sub-paragraphs 11.2 (b) in order to prevent customers from becoming victims of fraud.

S 11.2 A financial institution shall ensure that a customer shall not be held liable for losses arising from a credit transfer transaction unless the financial institution can prove on a balance of probabilities that–

(a) the customer has acted fraudulently;

(b) the customer has failed to carry out the following obligations as communicated by the financial institution to the customer in accordance with sub-paragraph 11.1(f):

(i) not deliberately disclosing the access identity (ID) and passcode to any other person;

(ii) taking reasonable steps to keep security device secure at all times; or

(iii) reporting a breach of the security of a passcode, the loss of a security device or any unauthorised transaction to the financial institution as soon as reasonably practicable, upon the customer becoming aware of the breach, loss or unauthorised transaction respectively.

Provisions applicable to approved e-money issuers

S 12.1 An approved e-money issuer–

(a) shall diversify the placement of the funds received from its customers in exchange of the e-money issued, in bank accounts to mitigate exposure to any single banking institution;

(b) shall not undertake any activity that has the object or effect of

circumventing the prohibition set out in paragraph 13.1 of the Bank's Guideline on Electronic Money on–

(iv) the issuance of e-money at a discount, i.e. issue e-money that has a monetary value greater than the sum received;

(v) the use of the money collected to extend credit to any other persons;

(vi) the extension of credit to the user, or payment of interest or profit on the e-money balances, or anything else that would add to the monetary value of the e-money; and

(vii) associating, linking or using the e-money scheme or platform to conduct illegal activities; and

(c) shall not use its e-money platform or system to promote or cross-sell any financial products except with BNM's prior written approval.

[The remainder of this page is intentionally left blank]

APPENDIX

Limits and requirements for CDD for e-money accounts

CDD requirement	Account functionality	Account limit	Transaction limit
No CDD	• Purchase transactions only • Cash-out/ withdrawal not allowed[9]	Less than RM5,000	• Less than RM3,000 per transaction • Up to RM50,000 per annum[10]
Simplified CDD Identify and verify the customer's identity by- • collecting customer's information[11]; • funding e-money account from a bank account or a payment card; and • verifying the customer's name or NRIC with a banking institution or an issuer of payment card.	• Purchase transactions • Fund transfers • Cash-out/ withdrawal not allowed[9]	Up to the account limit approved by the Bank	• Up to RM50,000 per annum[10] • No restriction on fund transfer to the customer's own bank account

[9] A customer is allowed to obtain a refund of the funds in his or her e-money account upon termination or closure of the e-money account. An approved issuer of e-money must ensure timely refund of its customer's funds in accordance with the requirement stipulated in the Guideline on E-Money.

[10] The permissible cumulative amount of funds that a customer can transfer to another e-money account within a calendar year.

[11] In accordance with paragraph 13.4.1 of the Bank's Guidelines on AML/CFT Sector 1 (Banking and Deposit-Taking Institutions) and paragraphs 13.4.1 and 13.4.2 of the Bank's Guidelines on AML/CFT Sector 4 (Electronic Money and Non-Bank Affiliated Charge & Credit Card).