HONG LEONG FINANCE DIGITAL TERMS & CONDITIONS

Thank you for your interest in the Digital Channels (as defined below) and the Digital Services (as defined below), which are provided by Hong Leong Finance Limited and its successors ("**HLF**", "**we**", "**our**" and "**us**") to its Account Holders (as defined below).

The following terms and conditions including the Appendices (these "**Digital Platform Terms**") set out the agreement between HLF and the Account Holder governing the Account Holder's access to and the use of the Digital Channels and the Digital Services. **By accessing and/or using the Digital Channels and/or the Digital Services, the Account Holder agrees to be bound by these Digital Platform Terms. If the Account Holder does not agree to these Digital Platform Terms, the Account Holder must not continue to access the Digital Channels or any of the Digital Services.**

PART 1 – DEFINITIONS AND INTERPRETATION

1. Definitions

1.1 In these Digital Platform Terms, unless the context otherwise requires:

1.1.1 "**Account**" means any account and/or joint account maintained by HLF including any savings account, fixed deposit account, business transactional current account, loan account and loan facilities account opened with HLF and any account maintained by us in relation to a hire purchase agreement;

1.1.2 "**Account Holder**" means the person in whose name an Account is maintained by HLF (whether as a single Account Holder or a joint Account Holder) and shall, where the context permits, include any legal and/or personal representative, successor-in-title and/or assign of such person;

1.1.3 "**Account Terms**" means HLF's prevailing Terms and Conditions Governing Accounts and Services available at the Portal, as amended from time to time, and any other prevailing terms and conditions governing use of HLF's facilities, services and/or the Account(s);

1.1.4 "**Affiliates**" means with respect to an entity, any person directly or indirectly Controlled by, Controlling or under common Control with that entity;

1.1.5 "**App**" means the mobile application known as "*HLF Mobile and Internet Services*" (or such other replacement name or additional name as may be prescribed by us from time to time);

1.1.6 "**Approved App Stores**" means (i) the official Apple App Store, currently designated by Apple Inc. as "App Store", accessible through such website, channel or other electronic means as Apple Inc. may prescribe from time to time; (ii) the official Google Play, currently designated by Google LLC as "Google Play", accessible through such website, channel or other electronic means as Google LLC may prescribe from time to time; and (iii) such other applications or websites as may be specified by HLF from time to time;

1.1.7 "**Confidential Information**" means HLF's confidential information and includes:

(i) all of HLF's financial, marketing, sales, technical, scientific, operational, commercial and human resource information, and all trade secrets, business plans, financial and/or contractual arrangements, product information, processes, formulas, designs, specifications, drawings, data, manuals and instructions; and

(ii) information of or relating to HLF, or relating to HLF's personnel, policies or business strategies of and information which HLF considers to be confidential or which HLF marks as confidential at the time of disclosure;

1.1.8 "**Content**" means text, software, code, scripts, webpages, music, sound, photographs, video, graphics, graphical user interface, forms, diagrams or other material contained in the App and/or the Portal;

1.1.9 "**Control**" or its derivatives or variants (i.e. "*Controlling, Controlled by or under the common Control*") means with regard to an entity the legal, beneficial or equitable ownership, directly or indirectly, of 50 per cent or more of the issued capital or voting rights (or other ownership interest, if not a corporation) of such entity, or the equivalent right under contract or otherwise, to control or cause the direction of management and policy decisions of such entity with regard to relevant subjects;

1.1.10 "**Digital Channels**" means the Portal and the App;

1.1.11 "**Digital Services**" means any services, products, programmes, modules, functionalities, features and/or facilities which HLF may make available from time to time via the Portal and/or the App;

1.1.12 "**Electronic Instructions**" means any communication, instruction, order, message, data, information or other materials received by HLF via the Digital Services and referable to the Account Holder's Security Codes (including use of the Security Codes by any person, whether authorised or unauthorised by the Account Holder), from the Account Holder or purporting to come from the Account Holder;

1.1.13 "**Electronic Statements**" means statements of accounts, information relating to the Account Holder's Electronic Instructions, confirmations of the Account Holder's Electronic Instructions and any other information relating to the Account that may be provided by HLF in an electronic form, through the Digital Services and/or such other channels as HLF may designate from time to time;

1.1.14 "**E-Payments Guidelines**" means the E-Payments User Protection Guidelines issued by the Monetary Authority of Singapore, as may be amended and supplemented from time to time, available on the official Monetary Authority of Singapore website or such other website as designated by the Monetary Authority of Singapore from time to time;

1.1.15 "**Face Recognition Features**" means such third party face recognition features designated as such by HLF from time to time which shall be deemed to include, unless otherwise notified by HLF, the face recognition feature of Apple's iOS and the face recognition feature of Google Android on devices that meet or exceed HLF's requirements;

1.1.16 "**Fingerprint Recognition Features**" means such third party fingerprint recognition features designated as such by HLF from time to time, and will be deemed to include, unless otherwise notified by HLF, the fingerprint recognition feature of Apple's iOS and the fingerprint recognition feature of Google Android on devices that meet or exceed HLF's requirements;

1.1.17 "**Guidelines**" has the meaning given in Clause 3.2.2;

1.1.18 "**high-risk activities**" has the meaning given in the E-Payment Guidelines;

1.1.19 "**HLF Indemnitees**" has the meaning given in Clause 17.1;

1.1.20 "**Intellectual Property Rights**" means all copyright, patents, utility innovations, trade marks and service marks, geographical indications, domain names, layout design rights, registered designs, design rights, database rights, trade or business names, rights protecting trade secrets and confidential information, rights protecting goodwill and reputation, and all other similar or corresponding proprietary rights and all applications for the same, whether presently existing or created in the future, anywhere in the world, whether registered or not, and all benefits, privileges, rights to sue, recover damages and obtain relief or other remedies for any past, current or future infringement, misappropriation or violation of any of the foregoing rights;

1.1.21 "**Joint Account**" means an Account in the joint names of two or more Account Holders;

1.1.22 "**Losses**" means all losses, liabilities, settlement sums, costs (including legal costs and costs of other professionals), charges, expenses, actions, proceedings, claims and demands, whether foreseeable or not;

1.1.23 "**Marks**" means the trade marks, symbols, service marks, trade names, logos and other proprietary designations used and displayed on any of the Digital Channels;

1.1.24 "**Personal Data**" has the same meaning as "personal data" as defined in the Singapore Personal Data Protection Act 2012;

1.1.25 "**Portal**" means the official Hong Leong Finance website, currently designated by HLF as "HLF Digital", and/or any other website that HLF may specify from time to time;

1.1.26 "**Prohibited Materials**" means any information, graphics, photographs, data and/or any other material that:

(i) contains any computer virus or other invasive or damaging code, program or macro;

(ii) infringes any third party Intellectual Property Rights or any other proprietary rights;

(iii) is defamatory, libellous or threatening;

(iv) is obscene, pornographic, indecent, counterfeited, fraudulent, stolen, harmful or otherwise illegal under the applicable law (including without limitation the provisions of the Singapore Broadcasting Authority (Class Licence) Notification 1996); and/or

(v) is or may be construed as offensive and/or otherwise objectionable, in HLF's sole opinion;

1.1.27 "**Protected Account**" means an Account that is a "protected account" as defined in the E-Payments Guidelines;

1.1.28 "**Protected Account Holder**" means the person in whose name a Protected Account is maintained by HLF (whether in the person's sole name or jointly with any other person(s)) and shall, where the context permits, include any legal and/or personal representative, successor-in-title and/or assign of such person;

1.1.29 "**Registered Mobile Devices**" means devices enabled with the Fingerprint Recognition Features or Face Recognition Features which have been registered with HLF for access and/or use of the Digital Services, in respect of any Account;

1.1.30 "**Records**" has the meaning given in Clause 9.9;

1.1.31 "**Security Codes**" means Singpass Access Credentials, the App on the Registered Mobile Device, any username, password, personal identification number, hardware or electronic token, and any other unique identification or credential (including any device, token, credential or password used in conjunction with multi-factor authentication procedures) either provided by the Account Holder or issued, prescribed, or otherwise approved by HLF, and allocated to the Account from time to time in order to enable the Account Holder to access and/or use the Digital Services, as communicated in the Guidelines;

1.1.32 "**Service Charges**" has the meaning given in Clause 11;

1.1.33 "**Singpass**" means the electronic identification, authentication, or authorisation service of the Government of Singapore known as "*Singpass*" through such devices, websites, channels or platform, as may be designated by the Government of Singapore from time to time;

1.1.34 "**Singpass Access Credentials**" means such authentication, configuration, use and/or access procedures of Singpass (such as Singpass Face Verification or passwords or passcodes that the Account Holder has set up for use with the Singpass Account) that have been enabled or used by HLF, or that have been incorporated by HLF into HLF's own authentication procedures, to identify the Account Holder and/or for the purposes of allowing access to and/or use of the Digital Services;

1.1.35 "**Singpass Account**" refers to the Account Holder's account, registered with the Government of Singapore for the purpose of using Singpass;

1.1.36 "**Singpass App**" means the mobile application designed to, amongst other things, be used as an authentication form factor, known as "*Singpass*" from Approved App Stores, and used in connection with Singpass and the Account Holder's Singpass Account;

1.1.37 "**Singpass Face Verification**" means the biometrics identification, authentication and authorisation service currently known as "*Singpass Face Verification*" that utilises facial recognition technology;

1.1.38 "**transaction notification threshold**" has the meaning given in the E-Payment Guidelines;

1.1.39 "**Taxes**" has the meaning given in Clause 12;

1.1.40 "**Third Party Materials**" has the meaning given in Clause 5.1; and

1.1.41 "**Third Party Terms**" has the meaning given in Clause 5.1.

2. Interpretation

2.1 In these Digital Platform Terms: (i) whenever the words "include", "includes" or "including" are used in these Digital Platform Terms, they will be deemed to be followed by the words "without limitation"; (ii) reference to Clauses, Paragraphs and Appendices are (unless otherwise stated) to clauses, paragraphs and appendices of these Digital Platform Terms; (iii) words importing the singular only shall also include the plural and vice versa where the context requires and references to persons include bodies incorporate or unincorporated, including partnerships and their successors and assigns; (iv) unless expressly indicated otherwise, all references to a number of days mean calendar days, and the words "month" or "monthly" as well as all references to a number of months means calendar months; (v) clause, paragraph and/or appendix headings are inserted for convenience only and shall not affect the interpretation of these Digital Platform Terms; and (vi) references to a statute, law, by-law, regulation, rule, directive, delegated legislation or order also refers to the same as amended, modified or replaced from time and to any by-law, regulation, rule, directive, delegated legislation or order made thereunder.

2.2 In addition to these Digital Platform Terms, the access and use of the Digital Channels and the Digital Services is also subject to HLF's Account Terms, which continue to apply with full force and effect. In the event of any conflict or inconsistency between these Digital Platform Terms and the Account Terms, the terms of these Digital Platform Terms shall prevail to the extent of the conflict or inconsistency.

PART 2 – GENERAL TERMS OF ACCESS AND USE

3. Conditions of access and use

3.1 **Provision of the Digital Services**: As part of HLF's ongoing efforts to improve convenience and accessibility, HLF is pleased to provide the Digital Services to its Account Holders on the terms and conditions set out in these Digital Platform Terms and subject to such Account Holders' completion of the application process.

3.2 **Additional terms and guidelines**: The Account Holder acknowledges and agrees that, in addition to these Digital Platform Terms:

3.2.1 the use of specific aspects of the Digital Channels and/or the Digital Services (including newly launched features or services of the Digital Services) offered by HLF may be subject to additional terms and conditions (including eligibility requirements), which will apply in full force and effect. In the event of any inconsistency between the Digital Platform Terms and any such additional terms and conditions, the additional terms and conditions shall prevail insofar as the inconsistency relates to the specific aspects of

the Digital Channels and/or the Digital Services in question unless otherwise provided; and

3.2.2 the Account Holder shall comply with any and all guidelines, notices, operating rules and policies and instructions pertaining to the access and/or use of the Digital Channels and/or the Digital Services (collectively, the "**Guidelines**"), as well as any amendments to the aforementioned Guidelines issued by HLF from time to time. HLF reserves the right to revise such Guidelines at any time and the Account Holder is deemed to be aware of and bound by any changes to the foregoing upon their publication on the Digital Channels.

3.3 **Digital Services may vary and may be accessed through different devices**: The Digital Services may be made available through different devices (such as kiosks or via applications on mobile devices) and further details on the access and use of the Digital Services through these devices may be provided in the Guidelines. The features of the Digital Services may also vary depending on the devices in question and access and use of the Digital Services may be subject to specific conditions of use that HLF prescribes. When accessing the Digital Services through a device not maintained by HLF, the Account Holder shall take reasonable steps to ensure that the device is secure, including at a minimum ensuring that:

3.3.1 the device's browser is updated to the latest version available;

3.3.2 the App is downloaded onto the device only from Approved App Stores;

3.3.3 the device's operating system is patched with all security updates provided by the operating system provider;

3.3.4 the device is only accessible by strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods made available by the device provider such as Face Recognition Features and Finger Recognition Features;

3.3.5 there is up-to-date anti-virus software installed and maintained on the device;

3.3.6 the device is not rooted or jailbroken; and

3.3.7 no applications from third-party websites outside official sources ("sideload applications") are downloaded and installed onto the device, in particular unverified applications which request device permissions that are unrelated to their intended functionalities.

3.4 **Restricted use**: Save where expressly provided for in these Digital Platform Terms, the Account Holder agrees and undertakes not to, whether directly or indirectly, do any of the following:

3.4.1 impersonate any person or entity or to falsely state or otherwise misrepresent his or her affiliation with any person or entity;

3.4.2 use the Digital Channels and/or the Digital Services for illegal purposes;

3.4.3 attempt to gain unauthorised access to or otherwise interfere or disrupt other computer systems or networks connected to the Digital Channels;

3.4.4 other than as expressly required by HLF, carry out any data mining, data compilation or data extraction (including of any Personal Data) for the purposes of statistical, trade or for other forms of analysis (and the development of derivative materials and works) on any aspect of HLF's business processes or practices or in relation to the Digital Channels;

3.4.5 collect and/or retain any Personal Data that may be accessible through and in relation to the Digital Channels;

3.4.6 post, promote or transmit through the Digital Channels any Prohibited Materials;

3.4.7 interfere with another Account Holder's utilisation and enjoyment of any of the Digital Channels and/or any of the Digital Services;

3.4.8 use or upload, in any way, any software or material that contains, or which the Account Holder has reason to suspect that contains, viruses, damaging components, malicious code or harmful components which may impair or corrupt the Digital Channels' data or damage or interfere with the operation of another Account Holder's Device;

3.4.9 reproduce, reverse engineer, decompile, disassemble, separate, alter, distribute, republish, display, broadcast, hyperlink, mirror, frame, transfer, transmit or install on any services, system or equipment (in any manner or by any means) any part(s) of the Digital Channels or the Content without HLF's prior written permission or that of the relevant copyright owners;

3.4.10 remove or obscure any proprietary notices (including copyright notices) in or on the Digital Channels and/or the Content;

3.4.11 use any of the Digital Channels other than in conformance with the acceptable use policies of any connected computer networks, any applicable Internet standards and any other applicable laws, or view, listen to, download, print or use the Digital Channels other than as allowed under applicable laws.

3.5 **Applicability of the E-Payments Guidelines**: The E-Payments Guidelines apply to HLF as a "responsible FI" in respect of Accounts which are Protected Accounts. Protected Account Holders will be "account holders" and "account users" as defined and referred to in the E-Payments Guidelines. The E-Payments Guidelines impose certain duties on "account holders" and "account users", as well as responsible FIs, as set out in Section 3 and Section 4 of the E-Payments Guidelines respectively. Sections 3 and 4 of the E-Payments Guidelines are reproduced in their entirety in the Appendix to these Digital Platform Terms. You must read the Appendix carefully and ensure that you understand and perform your duties and obligations thereunder. Failure to do so may result in you being liable for losses arising from unauthorised transactions or otherwise from the use of the Digital Services.

4. Reservation of rights

4.1 **Right, but not obligation, to monitor or control use or content, to report activity or request information**: HLF reserves the right, but shall not be obliged to:

4.1.1 monitor, screen or otherwise control any activity, Content or material on the Digital Channels. HLF may in its sole and absolute discretion, investigate any violation of these Digital Platform Terms and may take any action it deems appropriate;

4.1.2 prevent or restrict access of the Account Holder to any of the Digital Channels and/or Digital Services;

4.1.3 report any activity HLF suspects to be in violation of any applicable law, statute or regulation to the appropriate authorities and to co-operate with such authorities; and/or

4.1.4 request any information and data from the Account Holder in connection with such Account Holder's access to and/or use of the Digital Channels and/or Digital Services at any time and to exercise HLF's rights under this Clause 4.1.4 if the Account Holder refuses to divulge such information and/or data or if the Account Holder provides, or if HLF has reasonable grounds to suspect that the Account Holder has provided, inaccurate, misleading or fraudulent information and/or data.

4.2 **Availability of and modifications to the Digital Channels and/or the Digital Services**: HLF may, from time to time and without giving any reason or prior notice, upgrade, maintain, modify, alter, suspend, discontinue the provision of or remove (including downtime for the maintenance of the Portal), whether in whole or in part, the Digital Channel(s) and/or the Digital Services (including any Content contained therein), and shall not be liable if any such upgrade, maintenance, modification, alteration, suspension, discontinuance or removal prevents the Account Holder from accessing and/or using the Digital Channel(s), the Digital Services and/or any part thereof.

4.3 **Sub-contracting and delegation**: HLF reserves the right to delegate or sub-contract the performance of any of its functions in connection with Digital Channels and/or the Digital Services and reserves the right to use any service providers, subcontractors and/or agents on such terms as HLF may deem appropriate.

5. Third Party Materials

5.1 **Access to and/or use of Third Party Materials**: HLF may provide, facilitate or require, through the Digital Channels, access to or use of websites, software or services of third parties ("**Third Party Materials**"). Third Party Materials are provided by the relevant Third Parties and such access or use may be subject to additional terms and conditions imposed by third parties (the "**Third Party Terms**"). It is the Account Holder's responsibility to ensure compliance with any applicable Third Party Terms and the Account Holder is deemed to have notice of the same.

5.2 **No representations, endorsements etc. by HLF**: The Account Holder acknowledges and agrees that:

5.2.1 HLF makes no representations or warranties as to having reviewed or verified the relevance, timeliness, accuracy, adequacy, commercial value, completeness or reliability of any Third Party Materials;

5.2.2 any provision, facilitation or requirement, by HLF through Digital Channels, of access to or use of any Third Party Materials is not and does not imply, an endorsement by, association or affiliation with HLF or the verification by HLF of Third Party Materials;

5.2.3 Third Party Materials are not under HLF's control, and HLF is not liable for any errors, omissions, delays, defamation, libel, slander, falsehood, obscenity, pornography, profanity, inaccuracy or any other objectionable material contained in the contents, or the consequences of accessing, any Third Party Materials; and

5.2.4 the Account Holder's access to, use of and/or reliance on any Third Party Materials is solely at the Account Holder's own risk and HLF shall under no circumstances be responsible or liable for any Losses arising out of, or in connection with, such access, use and/or reliance.

6. Alerts and advertising

6.1 **Alerts**: The Account Holder may receive notification alerts in connection with the Account Holder's access and/or use of the Digital Channels, the Digital Services and/or the Content from time to time, such as, but not limited to, notifying the Account Holder of any unread messages or activity on the Account and notifying the Account Holder, on a real time basis, of all outgoing payment transactions, activation and creation of a Security Code and the conduct of any high-risk activities made from Protected Accounts. Such alerts may be notified by SMS, email, in-app/push notifications (i.e. mobile push notifications or pop-up screen in the App or the Account Holder's browser) and/or any other method of notification as may be determined by HLF from time to time. Alerts will be sent according to your chosen preferences (including any preferred transaction notification threshold). If you have not indicated any alert preferences, the alerts will be sent via our applicable default settings. We may amend the modes of sending alerts and we will inform you if this has an impact on your alert preferences. HLF does not guarantee the delivery, timeliness or accuracy of such alerts. HLF reserves the right to vary any alert (including the content thereof) without giving any reason or prior notice. Subject to Clause 15.4.5, HLF shall not be liable to the Account Holder or anyone else for Losses arising from:

6.1.1 non-delivery, delayed delivery or wrong delivery of an alert;

6.1.2 inaccurate content of an alert; or

6.1.3 use or reliance by the Account Holder or anyone else on the contents of an alert for any purpose.

6.2 **Enabling and monitoring transaction alerts for Protected Accounts**: Pursuant to the E-Payments Guidelines, it is the Protected Account Holder's responsibility to enable notification alerts on any device used to receive notification alerts from HLF in respect of a Protected Account, to opt to receive all notification alerts via SMS, email or in-app/push notification for all outgoing payment transactions (in accordance with the transaction notification threshold), activation and creation of any Security Code and the conduct of high-risk activities made from the Protected Account and to monitor the notification alerts sent to the Protected Account contacts. HLF assumes that the Protected Account Holder will monitor such notification alerts without further reminders or repeat alerts. Failure to enable and/or monitor notification alerts may result in the Protected Account Holder being liable for unauthorised payment transactions and/or losses arising out of or in connection with any unauthorised activity (as further described in Clause 15.4.1 below).

6.3 **Joint Accounts**. Where you are an Account Holder of a joint account, we may send alerts to you but not to the rest of the account holders (including any other account holders who have not signed up for the Digital Services).

6.4 **Advertising**: HLF may attach banners, java applets and/or such other Content or materials to the App and/or the Portal, including under the "Deals For You" module, for the purposes of advertising HLF's (or HLF's Affiliates') products and/or services. For the avoidance of doubt, the Account Holder shall not be entitled to receive any payment, fee and/or commission in respect of any such advertising or other promotional materials.

7. Joint Accounts

7.1 Where the Account is a Joint Account, these Digital Platform Terms shall be binding on the Account Holders in respect of such Joint Account jointly and severally.

7.2 If the Joint Account requires joint signatories, each of the Account Holders may be able to view, but will not have transactional capability over, such Joint Account through the Digital Channels and will be unable to issue Electronic Instructions in relation to such Joint Account. If the Joint Account only requires a single signatory, each of the Account Holders will be able to view such Joint Account through the Digital Channels and transact, give, authorise or issue Electronic Instructions in relation to such Joint Account, which HLF may choose to act upon.

7.3 Without prejudice to Clause 7.2 or any provision in the Account Terms, HLF is entitled to take any of the following steps in respect of any Joint Account without incurring responsibility for any Losses:

7.3.1 require all Account Holders of the Joint Account to provide consistent Electronic Instructions, or express consent in writing; or

7.3.2 decline to act upon any Electronic Instructions in respect of the Joint Account, including where contradictory instructions are provided by the Account Holders.

PART 3 – SECURITY CODES AND ELECTRONIC INSTRUCTIONS

8. Security Codes

8.1 **Use and issuance of Security Codes**: Security Codes are required for access to the Digital Services. HLF may at any time in its sole and absolute discretion forthwith invalidate any Security Codes without giving any reason or prior notice and shall not be liable or responsible for any loss or damage suffered by or caused by the Account Holder or arising out of or in connection with or by reason of such invalidation.

8.2 **Deemed use / access**: The Account Holder agrees to be bound by any access or use of the Digital Services (whether such access or use are authorised by the Account Holder or not) which are referable to the Account Holder's Security Codes. The Account Holder agrees and acknowledges that any use of or access to the Digital Services referable to the Account Holder's Security Codes and any Electronic Instructions shall be deemed to be, as the case may be:

8.2.1 use of or access to the Digital Services by the Account Holder; and

8.2.2 Electronic Instructions that the Account Holder had transmitted or validly issued.

8.3 **Responsibility for Security Codes**: The Account Holder may from time to time be required to change his or her Security Codes (including any username and/or password) and agrees to do so when required by HLF. The Account Holder shall keep his or her Security Codes confidential and take the necessary steps to prevent unauthorised disclosure of his or her Security Codes and shall be responsible for any disclosure or use (whether such use is authorised or not) of his or her Security Codes. Without limiting the foregoing, the Account Holder must not: (a) voluntarily disclose any Security Code to any third party, including any staff of HLF; (b) disclose the Security Code in a recognisable way on any payment account, authentication device or any container for the payment account; or (c) keep a record of any Security Code in a way that allows any third party to easily misuse the Security Code. The Account Holder must notify HLF immediately if he or she has knowledge that or has reason to suspect: (a) that the confidentiality of his or her Security Codes (including the Singpass Access Credentials) has been compromised; or (b) that there has been any unauthorised use of the same.

8.4 **Use of strong passwords as Security Codes**: Where the Account Holder is required to create a password as a Security Code, the Account Holder should select a numeric or alphabetical password that is strong, including, where possible a mixture of letters and numbers. The Account Holder must not use passwords that is easily recognisable, such as one which represents the Account Holder's birth date, or is part of the Account Holder's name. Please note that the use of easily recognisable passwords increases the risk of unauthorised use of such Security Codes, which could, in turn, lead to unauthorised payment transactions that will result in losses to the Account.

9. Account Holder's Electronic Instructions:

9.1 **Responsibility for accuracy, completeness and authenticity of the Electronic Instructions**: All Electronic Instructions provided by an Account Holder through the Digital Services shall be given in the manner indicated by HLF. The Account Holder is responsible for the accuracy, completeness and authenticity of the Electronic Instructions so provided to HLF.

9.2 **Electronic Instructions deemed to be irrevocable, etc.**: All Electronic Instructions will be deemed to be irrevocable, conclusive and unconditional upon transmission through the Digital Services unless HLF in its absolute discretion determines otherwise. Nevertheless, in certain circumstances Account Holder may request to cancel or amend the Electronic Instructions which HLF will endeavour to give effect to on a commercially reasonable effort basis. However, notwithstanding the foregoing, we are not obliged to give effect to any request to cancel or amend any Electronic Instruction.

9.3 **No obligation to investigate instructions / authority**: The Account Holder agrees and acknowledges that HLF is not required and are unable to verify or investigate the authenticity of, or authority of persons effecting, the Electronic Instructions. The Account Holder further agrees that HLF and its service providers shall be entitled (but not obliged to) (a) treat the Electronic Instructions as the Account Holder's authentic and duly authorised instructions, notwithstanding any error; fraud; forgery; lack of clarity; or misunderstanding in respect of terms of such Electronic Instructions, and (b) act upon, rely on and/or hold the Account Holder solely responsible and liable in respect of the Electronic Instructions, as if the same were carried out, transmitted, or issued by the Account Holder. HLF shall not be liable for any Losses the Account Holder may incur as a result of HLF so treating any such Electronic Instructions.

9.4 **Right to require further information and/or decline acting**: Notwithstanding Clause 9.3, HLF may:

9.4.1 decline or delay to act on or refrain from acting promptly upon the Electronic Instructions in order to verify the authenticity or correctness thereof or until HLF has carried out the verification measures that it requires;

9.4.2 require any Electronic Instructions to be confirmed in writing by the Account Holder before acting on the same,

and HLF shall not be liable for any Losses as a result of delayed performance or non-performance of the Electronic Instructions as a result of the above.

9.5 Unless otherwise provided, all Electronic Instructions are deemed "*instructions*" of the Account Holder (as such term is used in the Account Terms) and accordingly shall be subject to the Account Terms which will apply in full force and effect to all Electronic Instructions.

9.6 **Verification and security measures:** HLF is entitled at its sole discretion, but shall not be obliged, to implement additional verification measures or other conditions or security measures (for example, requiring the Account Holder to take additional steps to prove the Account Holder's identity or requiring the Account Holder to take additional steps to confirm or validate any transaction or activity conducted through the Account, or otherwise imposing any cooling off period before any transaction or activity may be conducted through the Account).

9.7 **Processing of the Electronic Instructions**: The Account Holder agrees and acknowledges that the Electronic Instructions provided through the Digital Services may not be processed immediately, around the clock or in a timely manner.

9.8 **Priority of Electronic Instructions**: HLF may in its sole discretion determine the order of priority in effecting the Electronic Instructions. If we receive an Electronic Instruction after the relevant cut-off time on a business day (as notified to you from time to time) or on a non-business day, we will treat the Electronic Instruction as being received on the next business day.

9.9 **Conclusiveness**: The Account Holder acknowledges and agrees that any records (including records of any telephone conversations or Electronic Instructions) relating to the Digital Services that have been maintained by HLF or HLF's service providers (all such records collectively, the "**Records**") are binding and conclusive on the Account Holder and are conclusive evidence of all instructions, communications, information and/or data (including any Electronic Instructions) received or sent by HLF. The Account Holder agrees that all such Records are admissible in evidence and that the Account Holder shall not challenge or dispute the admissibility, reliability, validity, accuracy or authenticity of such Records and hereby waives all of the Account Holder's rights (if any) to so challenge or object.

10. Account balance/transaction history

10.1 **Access to electronic statements, etc.**: To the extent that the Digital Services allow the Account Holder to access any Electronic Statements, the Account Holder acknowledges and agrees that delivery of an Electronic Statement is deemed to have taken place at the time that HLF made available the Electronic Statement, and not at the time the Electronic Statement is actually reviewed by the Account Holder. It is the Account Holder's responsibility to view and access their Electronic Statements in a timely manner, and immediately report any error or inaccuracy found therein. Save where an objection is raised within 10 days after the deemed delivery of the Electronic Statement, the Account Holder shall be deemed to have accepted the

Electronic Statement and all matters contained therein as true, accurate and binding on the Account Holder and have waived all rights to bring an action against HLF in respect of any error or omission.

PART 4 – CHARGES, FEES AND PAYMENTS

11. **Right to impose charges and/or fees:** HLF reserves the right to impose fees or charges for accessing and/or using the Digital Channels, the Digital Services and/or any part thereof ("**Service Charges**") (including but not limited to imposing Service Charges for the provision of Electronic Statements, or printed copies of such Electronic Statements at the Account Holder's request). HLF may vary or waive any Service Charges mentioned in any part of these Digital Platform Terms and/or the Guidelines.

12. **Payment of Taxes:** The Account Holder agrees to bear any prevailing taxes, duties and levies ("**Taxes**") incurred in connection with any Electronic Instructions (including any payment HLF is required by law to collect and make in respect of such Taxes).

13. **Mode of payment:** Any Service Charges, Taxes and/or any Losses suffered by HLF as a result of HLF's provision and/or the Account Holder's use of the Digital Services shall be payable by the Account Holder in any manner which HLF deems fit (including by debiting the Account). In the event that timely payment is not made (whether in whole or in part), the Account Holder undertakes to pay any applicable interest at such rates as determined by HLF.

14. **Currency conversion:** The Account Holder authorises HLF to effect any currency conversions at the rate determined by HLF and/or its service providers where an Electronic Instruction, or the debiting or crediting of any Account in connection with an Electronic Instruction or in connection with Clause 13, requires the conversion of currency.

PART 5 – WARRANTIES & DISCLAIMERS, EXCLUSIONS OF LIABILITY, LIMITATION OF LIABILITY AND INDEMNITIES

15. Disclaimers

15.1 **No representation or warranties**: The Digital Channels and Digital Services are provided on an "*as is*" and "*as available*" basis. No representations or warranties of any kind, implied, express or statutory, including the warranties of non-infringement of third party rights, title, merchantability, satisfactory quality or fitness for a particular purpose are given in conjunction with the Digital Channels or Digital Services. Without prejudice to the generality of the foregoing, HLF does not warrant:

15.1.1 the accuracy, reliability, timeliness, adequacy or completeness of all data and/or information contained in the Digital Channels or Digital Services;

15.1.2 that the Digital Channels or Digital Services will be provided uninterrupted, secure or free from errors or omissions, or that any identified defect will be corrected;

15.1.3 that the Digital Channels or Digital Services are free from any computer virus or other malicious, destructive or corrupting code, agent, program or macros; and

15.1.4 the security of any information transmitted by the Account Holder or to the Account Holder through the Digital Channels and Digital Services.

The Account Holder accepts the risk that any information transmitted or received through the Digital Channels or Digital Services may be accessed by unauthorised third parties and/or disclosed by HLF or HLF's officers, employees or agents to third parties purporting to be the Account Holder or purporting to act under the Account Holder's authority. HLF neither endorses nor assumes any responsibility for the contents of the Account Holder's transmissions or communications through the Digital Channels or Digital Services and the Account Holder is solely responsible therefor. Transmissions over the Internet may be subject to interruption, transmission blackout, delayed transmission due to internet traffic or incorrect data transmission due to the public nature of the Internet.

15.2 **No offer of products**: All data and/or information contained in the Digital Channels and/or provided through the Digital Services is provided for informational purposes only. The data and information therein are not intended as nor shall they be construed as financial, tax, legal, regulatory or other advice or as an offer, solicitation or recommendation of securities or other financial products. No consideration has been given to the specific investment objective, financial situation and particular needs of any specific person, and the information herein should not be used as a substitute for any form of advice. The Account Holder should seek his or her own independent investment, financial, tax, legal, regulatory or other advice before making an investment in the investments or products and consider whether the investment or product is suitable for him.

15.3 **At the Account Holder's own risk**: Subject to Clause 15.4.5, any risk of misunderstanding, error, loss, damage or expense resulting from the use of the Digital Channels or Digital Services is entirely the Account Holder's, and HLF or any of its agents, or any officer, director, agent, servant, or employee thereof shall not be liable therefor.

15.4 **Additional Terms for Protected Accounts**: This Clause 15.4 applies only to Protected Accounts.

15.4.1 Duties of Protected Account Holders: A Protected Account Holder is required to comply with all of the duties in Section 3 of the E-Payments Guidelines. In particular, a Protected Account Holder must:

(i) read the contents of messages containing access codes sent by HLF to the Protected Account Holder to verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities;

(ii) refer to official sources (for example, the Monetary Authority of Singapore's Financial Institutions Directory) or the Digital Channels to obtain the website addresses and phone numbers of HLF;

(iii) not click on links or scan any Quick Response ("**QR**") codes purportedly sent by HLF unless the Protected Account Holder is expecting to receive information on products and services via such links or QR codes from HLF. **HLF will not send any links or QR codes requiring the Protected Account Holder to provide any access code or perform any payment transaction or high-risk activity**;

(iv) read all risk warning messages sent by HLF, before proceeding to confirm the performance of high-risk activities, and be responsible for understanding the risks and implications of performing high-risk activities by accessing the Digital

Channels for more information or contact HLF directly. **Where a Protected Account Holder proceeds to perform the high-risk activities, he or she is deemed to have understood the risks and implications as presented by HLF**.

15.4.2 Kill switch: All Protected Accounts will have a "kill switch" function. Upon activation, HLF will block further mobile and online access to the Protected Account. The "kill switch" function can be activated in such manner as notified to the Protected Account Holder from time to time (including through the Digital Channels). A Protected Account Holder should activate the "kill switch" function as soon as practicable, after he or she is notified of any unauthorised transactions and has reason to believe that the Protected Account has been compromised, or if he or she is unable to contact HLF.

15.4.3 Liabilities of Protected Account Holder: Without prejudice to the generality of Clause 15.3, the Protected Account Holder is liable for actual loss arising from any unauthorised transaction with respect to a Protected Account where such Protected Account Holder does not comply with any of the duties in Section 3 of the E-Payments Guidelines, or where the Protected Account Holder's recklessness was the cause of the loss. Examples of conduct that constitutes recklessness and could lead to losses from unauthorised transactions include:

(i) storing Security Codes in a manner that can be easily accessed by any third party;

(ii) knowingly sharing or surrendering Security Codes to non-account users resulting in completed transactions;

(iii) ignoring notifications, alerts or warnings from HLF;

(iv) following instructions of third parties to open new accounts with HLF without a reasonable basis;

(v) retaining sideload applications which are unverified or request device permissions that are unrelated to their intended functionalities; and

(vi) selecting a numeric or alphabetical password that is easily recognisable, such as one which represents the Protected Account Holder's birth date, or part of the Protected Account Holder's name.

15.4.4 The Protected Account Holder shall, on request by HLF, provide HLF with any information HLF may reasonably require to determine whether the Protected Account Holder was reckless. For the avoidance of doubt, where any "account user" (as defined in the E-Payments Guidelines) consented to a transaction, such transaction will not be an unauthorised transaction even if the Protected Account Holder may not have consented to it.

15.4.5 The Protected Account Holder will not be liable for any loss arising from an unauthorised transaction with respect to a Protected Account if:

(i) the loss arises from any action or omission by HLF falling within sub-paragraphs (a) to (c) below and does not arise from any failure by the Protected

Account Holder to comply with any duty in Section 3 of the E-Payments Guidelines. For this purpose, the relevant actions or omissions are:

(a) fraud or negligence by HLF, its employee, its agent or any outsourcing service provider contracted by HLF to provide HLF's services through the Protected Account;

(b) non-compliance by HLF or its employee with any requirement imposed by the Monetary Authority of Singapore on HLF in respect of its provision of any financial service; and

(c) non-compliance by HLF with any duty set out in Section 4 of the E-Payments Guidelines; or

(ii) the first S$1,000 of loss arising from such unauthorised transaction if such loss arises from any action or omission by any third party not referred to in sub-paragraph (i)(a) to (c) above, and does not arise from any failure by the Protected Account Holder to comply with any duty in Section 3 of the E-Payments Guidelines.

15.5 **Unauthorised and erroneous transactions**: The following applies to unauthorised transactions and transactions where money has been (i) placed with or transferred to the wrong recipient; or (ii) received by the Account Holder incorrectly ("**erroneous transactions**").

15.5.1 An Account Holder who wishes to report any unauthorised activity or erroneous transaction with respect to an Account may do so through the HLF Customer Service Centre or by way of the Call Back Form available on the official HLF website.

15.5.2 An Account Holder shall report any unauthorised activity to HLF as soon as practicable, and no later than 30 calendar days after receipt of any notification alert for any unauthorised activity, e.g. transactions, high-risk activities, and the activation and creation of any Security Code, that has not been initiated by the Account Holder or with the Account Holder's consent.

15.5.3 Any claim made by an Account Holder in relation to any unauthorised activity with respect to an Account shall be subject to HLF's assessment and claim resolution process, which will be communicated to the Account Holder at the relevant time.

16. Exclusions of liability

16.1 HLF or any of its agents, or any officer, director, agent, servant, or employee thereof shall in no event be liable to the Account Holder or and other person for any loss, damage, fines or claims (including any direct, indirect, incidental, special, consequential or punitive damages or economic loss or any claims for damage to property, loss of profits or loss of use), whatsoever or howsoever caused regardless of the form of action (including tort or strict liability) arising directly or indirectly from or in connection with the Digital Channels or Digital Services or any of the following:

16.1.1 any access, use or inability to access or use the Digital Channels or Digital Services;

16.1.2 any reliance on any data or information made available through the Digital Channels or Digital Services (including any error, omission or delay therein and misinterpretation of such data or information);

16.1.3 any system, server or connection failure, error, omission, delay, interruption, interception, delay in transmission or computer virus or other malicious, invasive, disruptive, corrupting or damaging code, agent, program or macros;

16.1.4 any use of or access to any other third party website, service, data, application, software, servers or source code linked to or accessed from the Digital Channels or Digital Services;

16.1.5 any services, information, data, software or material obtained or downloaded through the Digital Channels or Digital Services or from any other website or webpage provided through the Digital Channels or Digital Services or from any other party referred through the Digital Channels or Digital Services; and

16.1.6 any "jailbreak", "rooting", modification of, or the installation of illegitimate software or sideload applications (including, in particular, unverified applications which request device permissions that are unrelated to their intended functionalities) on any Registered Mobile Device,

whether foreseeable or not and even if HLF was advised of the possibility of such loss, damage, fines or claims.

16.2 **No provision of Internet access or other telecommunication services**: The Account Holder agrees and acknowledges that these Digital Platform Terms, the Digital Channels and the Digital Services do not include the provision of Internet access or other telecommunication services by HLF. Any Internet access or telecommunications services (such as mobile data connectivity) required by the Account Holder to access and use the Digital Channels and/or the Digital Services shall be the Account Holder's sole responsibility and shall be separately obtained by the Account Holder, at his or her own cost, from the appropriate telecommunications or internet access service provider.

17. Indemnification

17.1 Without limiting the generality of any provision in these Digital Platform Terms, the Account Holder shall indemnify, defend and hold harmless HLF or any of its agents, or any officer, director, agent, servant, or employee thereof (referred to as the "**HLF Indemnitees**") from and against any and all losses, damages, fines or claims which the HLF Indemnitees may suffer, sustain or incur, or which may be instituted, made, brought, threatened, alleged or established against the HLF Indemnitees, by any person and which in any case arises (whether directly or indirectly) out of, in relation to or by reason of:

17.1.1 any negligent and/or reckless act or omission, or any fraud, wilful default or wilful misconduct of the Account Holder;

17.1.2 the Account Holder's breach of or failure or delay in complying with any applicable laws, including any rules, code of conduct and/or guidelines issued by any governmental, administrative or regulatory authority or agency;

17.1.3 the Account Holder's breach of or failure or delay in complying with these terms;

17.1.4 the use, misuse or purported use or misuse of the Digital Channels and/or Digital Services by the Account Holder; and/or

17.1.5 anything done or omitted to be done by the Indemnified Persons pursuant to or in connection with any Electronic Instructions by the Account Holder;

17.1.6 the preservation or enforcement of HLF's rights as a result of the Account Holder's non-compliance with any term of these Digital Platform Terms.

17.1.7 any claims brought or threatened by a third party against any of the HLF Indemnitees from the circumstances specified in sub-clauses 17.1.1 to 17.1.6 of this Clause or any claims, causes of actions or demands by such third parties arising out of or in connection with the performance of these Digital Platform Terms.

PART 6 – INTELLECTUAL PROPERTY

18. Intellectual Property

18.1 **Ownership**: The Intellectual Property Rights in and to the Digital Channels and the Content are owned, licensed to, or controlled by HLF, its service providers or its licensors.

18.2 **Marks**: The Marks are those of HLF or third parties. Nothing on the Digital Channels and in these Digital Platform Terms shall be construed as granting, by implication, estoppel, or otherwise, any license or right to use (including as a meta tag to any other website) any Marks displayed on the Digital Channels, without HLF's written permission or any other applicable owner.

18.3 **Licence for personal and non-commercial purposes**: HLF grants the Account Holder a revocable, non-exclusive, non-transferable, non-sub-licensable, limited licence to use the Digital Channels and the Content for the Account Holder's personal and non-commercial purposes (including viewing, printing or using the Content for such purposes), subject to these Digital Platform Terms and all other applicable terms and conditions.

18.4 **Material submitted through the Digital Channels**: In relation to any information or material submitted by the Account Holder to HLF using the Digital Channels, the Account Holder hereby grants to HLF a royalty-free, perpetual, irrevocable, assignable, transferable, sub-licensable right and licence to use such information or material for any purpose it deems appropriate, including without limitation, the copying, modification, transmission, distribution and publication thereof, unless restricted by applicable laws. The Account Holder represents and warrants that such information or material submitted by the Account Holder does not infringe the rights of any other third party.

PART 7 – PERSONAL DATA AND CONFIDENTIALITY

19. Personal Data

19.1 The Account Holder consents to the collection, use, and disclosure of any Personal Data relating to, or provided by, the Account Holder, in accordance with HLF's Data Protection Notice at the Portal, the Account Terms, the Guidelines and any other terms and conditions notified by HLF.

20. Confidentiality

20.1 The Account Holder shall treat as confidential the Confidential Information and shall not divulge any Confidential Information to any person without HLF's prior written consent. The Account Holder shall take all reasonable precautions in dealing with any Confidential Information and shall establish and maintain sufficient security measures and procedures to provide for the safe custody of the Confidential Information and prevent unauthorised access thereto or use thereof.

20.2 Without prejudice to any other provision of these Digital Platform Terms, the Account Holder warrants and undertakes that the Account Holder will not license, publish, exploit or deal with the Confidential Information in any form (including in aggregated form).

20.3 Without in any way limiting any consent granted under any other agreement between Account Holder and HLF, the Account Holder hereby consents for HLF to disclose any information relating to the Account Holder or the Account Holder's Account to any of HLF's subsidiaries, branches, agents, service providers, subcontractors, correspondents, agencies and representative offices which has a legitimate business purpose for obtaining such information, including use in connection with the provision of the Digital Channels and Digital Services to the Account Holder and the operation, maintenance and support of Digital Channels and Digital Services and the features and functions made available therein.

20.4 The Account Holder's obligations under this Clause 20 shall survive the expiry or termination of these Digital Platform Terms.

PART 8 – TERMINATION AND EFFECTS OF TERMINATION

21. Termination or suspension of access and/or use by HLF

21.1 In HLF's sole and absolute discretion, HLF may at any time with immediate effect, without giving any reason or prior notice to the Account Holder, suspend, disable or restrict the access and/or use to the Digital Channels, the Digital Services, any Account and/or Security Codes (or any part thereof). Examples where this may occur include, but are not limited to the following:

21.1.1 when the Account Holder submits a request to HLF (for HLF's consideration) and HLF may exercise its sole and absolute discretion to suspend his or her Account; and

21.1.2 to prevent any misconduct, fraud, unlawful or criminal activity or omission via the use of any Account, notwithstanding whether HLF suspects any of the aforementioned.

21.2 In HLF's sole and absolute discretion, HLF may, at any time with immediate effect upon giving the Account Holder notice, terminate these Digital Platform Terms, without liability to the Account Holder whatsoever, for any reason whatsoever (including the Account Holder's breach of any of these Digital Platform Terms), or where if HLF believes that the Account Holder has violated or acted inconsistently with any terms or conditions set out herein, or if in HLF's opinion or the opinion of any regulatory authority, HLF is not suitable to continue providing the Digital Channels or Digital Services.

22. Termination by customer

22.1 An Account Holder may request for termination of his or her access to the Digital Channels or Digital Services at any time by giving a written notice of at least 14 days to HLF. The Account

Holder will remain responsible for any Electronic Instructions made in or through the Digital Channels or Digital Services prior to the effective date of such termination.

23. Effects of termination

23.1 Upon any termination of these Digital Platform Terms (by either the Account Holder or HLF):

23.1.1 all rights and/or licenses granted to the Account Holder under these Digital Platform Terms shall immediately cease and terminate;

23.1.2 the Account Holder must immediately stop any access or use of the Digital Channels, and HLF is entitled to immediately discontinue or terminate, the Account Holder's Account; the Account Holder's Security Codes; and the Account Holder's use of the Portal;

23.1.3 the Account Holder shall pay HLF all unpaid fees or charges accrued up to the date of termination; and

23.1.4 provisions of these Digital Platform Terms which are expressly stated to, or by their nature are intended to survive termination of these Digital Platform Terms, will continue to apply in accordance with their terms.

23.2 Termination will not affect any rights or obligations accrued prior to the effective date of termination or any obligations under these Digital Platform Terms which are meant to survive the termination.

PART 9 – GENERAL

24. Notices

24.1 **Notices from HLF**: All notices or other communications given to the Account Holder if:

24.1.1 communicated through any print or electronic media as HLF may select will be deemed to be notified to the Account Holder on the date of publication or broadcast; or

24.1.2 sent by post or left at the Account Holder’s address registered with HLF will be deemed to be received by the Account Holder on the day following such posting or on the day when it was so left.

24.2 **Notices from the Account Holder**: The Account Holder may only give notice to HLF in writing sent to HLF’s designated address or e-mail address, or via a call to the designated telephone number (calls may be recorded), and HLF shall be deemed to have received such notice only upon receipt. While HLF endeavours to respond promptly to notices from the Account Holder, HLF cannot guarantee that HLF will always respond with consistent speed. The designated mode of service of notices on HLF is:

Designated address: 16 Raffles Quay #01-05 Singapore 048581

Designated telephone number: 6579 6777

Designated callback arrangement process: If the Account Holder wishes to arrange a call back, the Account Holder may do so using the Call Back Form on the “Contact Us” webpage on HLF’s official website.

24.3 **Other modes**: Notwithstanding Clauses 24.1 and 24.2, HLF may from time to time designate other acceptable modes of giving notices (including but not limited to e-mail or other forms of electronic communication) and the time or event by which such notice shall be deemed given.

25. **Amendments**: HLF may by notice through the Digital Channels, or by such other method of notification as HLF may designate (which may include notification by way of e-mail), vary the terms and conditions of these Digital Platform Terms, such variation to take effect on the date HLF specifies. If the Account Holder uses the Digital Channels and Digital Services after such date, the Account Holder is deemed to have accepted such variation. If the Account Holder does not accept the variation, the Account Holder must stop accessing or using the Digital Channels and Digital Services and terminate these Digital Platform Terms. HLF's right to vary these Digital Platform Terms in the manner aforesaid may be exercised without the consent of any person or entity who is not a party to these Digital Platform Terms.

26. **Force majeure**: HLF shall not be liable for non-performance, error, interruption or delay in the performance of its obligations under these Digital Platform Terms (or any part thereof) or for any inaccuracy, unreliability or unsuitability of the Digital Channel or Digital Services or their contents if these are due, in whole or in part, directly or indirectly to an event or failure which is beyond HLF's reasonable control.

27. **Governing law and jurisdiction**: These Digital Platform Terms shall be governed and construed in all respects in accordance with the laws of Singapore. The Account Holder agrees to irrevocably submit to the exclusive jurisdiction of the courts of Singapore. HLF may (but shall not be obliged to) initiate and take any action or proceeding or otherwise against the Account Holder in Singapore or elsewhere as HLF in its discretion deems fit, and/or take concurrent legal proceedings in more than one country.

28. **No waiver**: In the event of a breach of these Digital Platform Terms by the Account Holder, HLF's failure to enforce these Digital Platform Terms shall not constitute a waiver of these terms, and such failure shall not affect the right later to enforce these Digital Platform Terms. HLF would still be entitled to use its rights and remedies in any other situation where the Account Holder breaches the Digital Platform Terms.

29. **Severability**: The invalidity or unenforceability of any of the provisions in these Digital Platform Terms shall not adversely affect or impair the validity or enforceability of the remaining provisions of these Digital Platform Terms.

30. **Cumulative rights and remedies**: HLF's rights and remedies under these Digital Platform Terms are cumulative and not exclusive of any rights or remedies provided by law or under any agreement.

31. **Rights of third parties**: Save as expressly provided, a person who is not a party to these Digital Platform Terms shall have no rights under the Contracts (Rights of Third Parties) Act 2001 of Singapore or other similar laws to enforce any term of these Digital Platform Terms, regardless of whether such person or entity has been identified by name, as a member of a class or as answering a particular description. For the avoidance of doubt, nothing in this Clause shall affect the rights of any permitted assignee or transferee of these Digital Platform Terms.

32. **Assignment**: The Account Holder may not assign its rights under these Digital Platform Terms without HLF's prior written consent. HLF may assign its rights under these Digital Platform Terms to any third party.

Appendix to the Digital Platform Terms

Sections 3 and 4 of the E-Payments Guidelines (last revised on 25 October 2024) are reproduced in their entirety below, together with the definitions of relevant terms as set out in the E-Payments Guidelines. The E-Payments Guidelines shall apply to all Protected Account Holders, in respect of Protected Accounts. For the purposes of the Protected Accounts, you will be the "account holder" and an "account user" referred to in the E-Payments Guidelines; any person you have authorised to give instructions to us (HLF) on your behalf with respect to the Protected Account will be an “account user”; and we (HLF) will be the "responsible FI" referred to in the E-Payments Guidelines.

The complete E-Payments Guidelines are available on the official Monetary Authority of Singapore website.

3 Duties of account holders and account users

Account holder to provide contact information, opt to receive all outgoing transaction notifications and monitor notifications

3.1 The account holder of a protected account should provide the responsible FI with contact information as required by the responsible FI in order for the responsible FI to send the account holder notification alerts for transactions, activation of digital security token and the conduct of high-risk activities in accordance with Section 4. Where the protected account is a joint account, the account holders should jointly give instructions to the responsible FI on whether the responsible FI should send transaction notifications under paragraphs 4.10 and 4.11 to any or all the account holders. The duties of the account holders in this Section 3 will apply to all the account holders that the responsible FI has been instructed to send transaction notifications to.

3.2 The account holder should at a minimum provide the following contact information which must be complete and accurate, to the responsible FI:

(a) where the account holder has opted to receive notification alerts by SMS, his Singapore mobile phone number; or

(b) where the account holder has opted to receive notification by email, his email address.

3.3 It is the account holder’s responsibility to enable notification alerts on any device used to receive notification alerts from the responsible FI, to opt to receive notification alerts via SMS, email or in-app/push notification for all outgoing payment transactions (of any amount that is above the transaction notification threshold), activation of digital security token and the conduct of high-risk activities made from the account holder’s protected account, and to monitor the notification alerts sent to the account contact. The responsible FI may assume that the account holder will monitor such notification alerts without further reminders or repeat notifications.

Account user to protect access codes

3.4 An account user of a protected account should not do any of the following:

(a) voluntarily disclose any access code to any third party, including the staff of any responsible FI;

(b) disclose the access code in a recognisable way on any payment account, authentication device, or any container for the payment account; or

(c) *keep a record of any access code in a way that allows any third party to easily misuse the access code.*

3.5 *If the account user keeps a record of any access code, he should make reasonable efforts to secure the record, including:*

(a) *keeping the record in a secure electronic or physical location accessible or known only to the account user; and*

(b) *keeping the record in a place where the record is unlikely to be found by a third party.*

Account user to secure access to protected account

3.6 *An account user of a protected account should at the minimum do the following where a device is used to access the protected account:*

(a) *download the responsible FI's mobile application(s) only from official sources[1];*

(b) *update the device's browser[2] to the latest version available;*

(c) *patch the device's operating systems[3] with regular security updates provided by the operating system provider;*

(d) *install and maintain the latest anti-virus software on the device, where applicable[4];*

(e) *use strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods made available by the device provider such as facial recognition or fingerprint authentication methods;*

(f) *not root or jailbreak the devices used; and*

(g) *not download and install applications from third-party websites outside official sources ("**sideload apps**"), in particular unverified applications which request device permissions that are unrelated to their intended functionalities.*

3.7 *An account holder should inform all account users of the security instructions or advice provided by the responsible FI to the account holder. An account user should where possible follow security instructions or advice provided by the responsible FI to the account holder.*

Account user to read content sent with access codes before completing payment transactions or high-risk activities

3.8 *An account user of a protected account should read the content of the messages containing the access codes[5] and verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities.*

[1] Examples: Apple App Store, Google Play Store
[2] Examples: Chrome, Safari, Internet Explorer, Firefox
[3] Examples: Windows operating system (OS), Macintosh OS, iOS, Android OS
[4] Examples: periodic updates, patches, version releases initiated by the antivirus software providers from time to time
[5] Examples include one-time passwords sent via SMS or equivalent push notifications via the official mobile application of the responsible FI

Account user to refer to official sources to obtain website addresses and phone numbers

*3.9 An account user of a protected account should refer to official sources, e.g., the MAS Financial Institutions Directory ("**FID**")[6], and the responsible FI's mobile application or the back of cards, e.g. credit card, debit card or charge card ("**official sources**") to obtain the website addresses and phone numbers ("**contact details**") of the responsible FI.*

3.10 To contact the responsible FI, an account user should use the contact details that were obtained from official sources.

*3.11 An account user should not click on links or scan Quick Response codes ("**QR codes**") purportedly sent by the responsible FI unless he is expecting to receive information on products and services via these links or QR codes from the responsible FI. The contents of these links or QR codes should not directly result in the account holder providing any access code or performing a payment transaction or high-risk activity.[7]*

Account user to understand the risks and implications of performing high-risk activities

3.12 An account user of a protected account should read the risk warning messages sent by the responsible FI before proceeding to confirm the performance of high-risk activities.

3.13 If an account user does not understand the risks and implications of performing high-risk activities, he should access the responsible FI's website for more information on these activities or contact the responsible FI prior to performing these activities. When the account user proceeds to perform the high-risk activities, he is deemed to have understood the risks and implications as presented by the responsible FI.

Account holder to report unauthorised activities on his protected account

3.14 The account holder of a protected account should report any unauthorised activity to the responsible FI as soon as practicable, and no later than 30 calendar days after receipt of any notification alert for any unauthorised activity, e.g., transactions, high-risk activities, and the activation of a digital security token, that has not been initiated by the account holder or with the account holder's consent.

3.15 Where the account holder is not able to report the unauthorised activity to the responsible FI as soon as he receives any notification alert for any unauthorised activity or within the time period set out in paragraph 3.14, the account holder should if the responsible FI so requests, provide the responsible FI with reasons for the delayed report.

The report should be made in any of the following ways:

(a) by reporting the unauthorised transaction to the responsible FI in any communications channel for such purpose as set out in the account agreement;

(b) by reporting the unauthorised transaction to the responsible FI in any other way and where the responsible FI acknowledges receipt of such a report.

[6] Website link: https://eservices.mas.gov.sg/fid

[7] Such links are only to provide information and could be part of regulatory requirements, such as Terms and Conditions, product description, steps to execute a transaction and fact sheet for investment products.

*Account holder to activate self-service feature ("**kill switch**") provided by the responsible FI promptly to block further mobile and online access to the protected account*

3.17 The account holder of a protected account should activate the kill switch provided by the responsible FI to block further mobile and online access to the protected account as set out in paragraph 4.14, as soon as practicable, after he is notified of any unauthorised transactions and has reason to believe that the account has been compromised, or if he is unable to contact the responsible FI.

Account holder to provide information on unauthorised transaction

3.18 The account holder of a protected account should within a reasonable time provide the responsible FI with any of the following information as requested by the responsible FI:

(a) the protected account(s) affected, including the account holder's affected accounts with other FIs if any;

(b) the account holder's identification information;

(c) the type of authentication device, access code and device used to perform the payment transaction;

(d) the name or identity of any account user for the protected account;

(e) whether a protected account, authentication device, or access code was lost, stolen or misused and if so:
- *the date and time of the loss or misuse,*
- *the date and time that the loss or misuse, was reported to the responsible FI, and*
- *the date, time and method that the loss or misuse, was reported to the police;*

(f) where any access code is applicable to the protected account,
- *how the account holder or any account user recorded the access code, and*
- *whether the account holder or any account user had disclosed the access code to anyone; and*

(g) any other relevant information about the unauthorised transaction that is known to the account holder, such as:
- *a description of the scam incident, including details of the communications with the suspected scammer(s);*
- *details of the remote software downloaded (if any) as instructed by the scammer(s);*
- *whether the account holder has received any OTPs and/or transaction notifications sent by the responsible FI, and where applicable/possible a confirmation from telecommunication operators to verify the receipt status only if the account holder is able to obtain it; and*
- *suspected compromised applications (if any) in the account user's device.*

Account holder to make police report

3.19 The account holder of a protected account should make a police report as soon as practicable if the responsible FI requests such a report to be made to facilitate its claims investigation process, or if the account holder suspects that he is a victim of scam or fraud.

3.20 The account holder should cooperate with the Police and provide evidence[8], as far as practicable. The account holder should also furnish the police report to the responsible FI within 3 calendar days of the responsible FI's request to do so, in order to facilitate the responsible FI's claims investigation process as set out in paragraph 4.22.

4 Duties of the responsible FI

4.1 Section 4 does not apply to any responsible FI in respect of any credit card, charge card or debit card issued by the responsible FI, except for paragraphs 4.2 to 4.6, 4.10 to 4.12, and 4.14 to 4.16.

Responsible FI to clearly inform account holder of user protection duties

4.2 A responsible FI should inform every account holder of a protected account of the user protection duties, including providing such information on its website or mobile application, and in the Terms and Conditions provided to an account holder for any new protected account issued.

4.3 For the purpose of paragraph 4.2 user protection duties comprise:

(a) duties of the account holder and account user as set out in Section 3; and
(b) duties of the responsible FI as set out in Section 4, excluding this paragraph.

Responsible FI to not send clickable links or QR codes via email or SMS, or phone numbers via SMS to account user

4.4 The responsible FI should not send clickable links or QR codes via email or SMS to an account user of a retail protected account unless:

(a) it is a link or QR code that only contains information for the account user and does not lead to a (i) website where the account user provides his access codes or performs any payment transaction or (ii) platform where the account user is able to download and install apps; and

(b) the account user is expecting to receive the email or SMS from the responsible FI.

4.5 A responsible FI should not send phone numbers via an SMS to an account holder of a protected account unless the account holder is expecting to receive the SMS from the responsible FI.

4.6 A responsible FI should ensure its website address is listed on MAS' FID, and that its contact details reflected on MAS' FID and other official sources are up to date.

Responsible FI to impose a cooling off period when performing high-risk activities

*4.7 A responsible FI should impose a cooling off period of at least 12 hours[9] where high-risk activities cannot be performed ("**cooling off period**"), when a digital security token is activated on a device, or when there is a login to a protected account issued by a relevant payment*

[8] For example, consumer can furnish his mobile device to the Police for forensics investigation.
[9] If the activation of the security token is via a non-straight through process (e.g. mailing of registration code), the duration of the non-straight through process counts towards fulfilling the cooling off period.

service provider on a new device.

Responsible FI to inform account user of the risks and implications of performing high-risk activities

4.8 A responsible FI should inform the account user of a protected account of the risks and implications of performing high-risk activities and obtain additional customer confirmation, at the point before the account holders perform the high-risk activities.

Responsible FI to provide notification alerts on a real time basis, for activation of digital security token and conduct of high-risk activities

4.9 The responsible FI should provide notification alerts on a real-time basis, that fulfil the following criteria, to the account holder of a protected account, when his digital security token is activated and any high-risk activities are performed:

(a) The notification alert should be sent to the account holder's existing account contact with the responsible FI. If the account holder has provided more than one account contact to the responsible FI, the notification should be sent to every account contact selected by the account holder to receive such notifications.

(b) The notification alert should be conveyed to the account holder by way of SMS, email or in-app/push notification.

(c) The notification alert should contain details relevant to the digital security token provisioning and activation or high-risk activity, such as information on the payee added, new transaction limits or a change in contact details.

(d) The notification alert should contain a reminder for the account holder to contact the responsible FI if the digital security token provisioning and activation or high-risk activity was not performed by the account holder.

Responsible FI to provide outgoing transaction notification alerts on a real-time basis

4.10 Subject to paragraph 4.11, a responsible FI should provide transaction notification alerts that fulfil the following criteria to each account holder of a protected account that the responsible FI has been instructed to send transaction notification alerts to in accordance with paragraph 3.1, in respect of all outgoing payment transactions (in accordance with the transaction notification threshold) made from the account holder's protected account.

(a) The transaction notification alert should be sent to the account holder's account contact. If the account holder has provided more than one account contact to the responsible FI, the transaction notification alert should be sent to every account contact selected by the account holder to receive such notifications.

(b) The transaction notification alert should be sent on a real time basis for each transaction.

(c) The transaction notification alert should be conveyed to the account holder by way of SMS, email, or in-app/push notification.

(d) The transaction notification alert should contain the following information, but the responsible FI may omit any confidential information provided that the information

provided to the account holder still allows the account holder to identify the transaction as being an authorised transaction (as referred to in paragraph 5.3) or unauthorised transaction.

- *Information that allows the account holder to identify the protected account such as the protected account number;*
- *Information that allows the account holder to identify the recipient whether by name or by other credentials such as the recipient's account number;*
- *Information that allows the responsible FI to later identify the account holder, the protected account, and the recipient account such as each account number or name of the account holder;*
- *Transaction amount (including currency);*
- *Transaction time and date;*
- *Transaction type;*
- *If the transaction is for goods and services provided by a business, the trading name of the merchant and where possible, the merchant's reference number for the transaction.*

Compliance with account holder's preference

4.11 Notwithstanding paragraph 4.10, a responsible FI can elect to comply with an account holder's transaction notification alert preferences. While the responsible FI should make available to account holders the option to receive transaction notification alerts for all outgoing payment transactions (of any amount) made from the account holder's protected account, if the account holder instructs or has instructed the responsible FI otherwise, the responsible FI should provide notification alerts for outgoing transactions in accordance with the account holder's instructions. For example, the responsible FI may provide outgoing transaction notification alerts to the account holder for amounts higher than $0.01 or only for certain types of outgoing transactions, as instructed by the account holder.[10]

4.12 A responsible FI should make available on its website or mobile application information on how an account holder can adjust the transaction notification settings. The responsible FI should explain how the liability of the account holder under Section 5 of the Guidelines may be affected by the account holder's transaction notification preferences and how any relevant claim by an account holder (as defined in paragraph 4.22) will be resolved. The responsible FI should act fairly and responsibly to the account holder at all times.

Incoming transaction notification alerts

4.13 A responsible FI is encouraged to provide transaction notification alerts that fulfil the criteria set out in paragraph 4.10(a) to (d) for payments to the account holder's protected account ("incoming transaction notifications") as a matter of good practice, as incoming transaction notification alerts provide e-payment users with a fuller view of their e-payments.

*Responsible FI to provide a self-service feature ("**kill switch**") for account holder to promptly block further access to protected account*

4.14 A responsible FI should provide a kill switch for an account holder to promptly block further mobile and online access to his protected account[11]. This includes disallowing mobile and online

[10] For example, if the account holder chooses not to receive pre-authorised, first person, or recurring transaction notifications, while the responsible FI should make the option to receive these notifications available to the account holder, the responsible FI may comply with the account holder's instructions and not notify the account holder of such transactions.
[11] Existing mobile and online banking session(s) are to be terminated as well.

payment transfers to third parties who are not authorised billers[12]. The kill switch should be made available in a prominent manner via the mobile application of the responsible FI, the automated teller machines ("ATMs") of the responsible FI, or the reporting channel provided by the responsible FI under paragraph 4.19 to report unauthorised transactions.

4.15 A responsible FI should educate every account holder of a protected account how to activate this feature, and highlight the duties of the account holder in paragraph 3.17 on when they should activate this feature.

Responsible FI to provide information to allow identification of payment recipient

4.16 A responsible FI should provide the following information accompanying the access codes[13] in the same message sent to the account user to allow the account user of a protected account to identify payment recipient:

(a) information that allows the account user to identify the protected account such as the protected account number;

(b) information that allows the account user to identify the recipient whether by name or by other credentials;

(c) the intended transaction amount (including currency); and

(d) a warning to remind the account user not to reveal the access code to anyone.

Responsible FI to provide recipient credential information

4.17 Where transactions are made by way of internet banking, any mobile phone application or device arranged for by a responsible FI for payment transactions, including a payment kiosk, a responsible FI should provide an onscreen opportunity for any account user of a protected account to confirm the payment transaction and recipient credentials before the responsible FI executes any authorised payment transaction.

4.18 The onscreen opportunity should contain the following information:

(a) information that allows the account user to identify the protected account to be debited;

(b) the intended transaction amount;

(c) credentials of the intended recipient that is sufficient for the account user to identify the recipient, which at the minimum should be the recipient's phone number, identification number, account number or name as registered for the purpose of receiving such payments; and

(d) a warning to ask the account user to check the information before executing the payment transaction.

Responsible FI to provide reporting channel

[12] Examples of payment transfers to authorised billers include pre-authorised transfers such as GIRO payments to billing organisations.
[13] Examples include one-time passwords (OTP) sent via SMS or equivalent push notifications via the official mobile application of the responsible FI

4.19 The responsible FI should provide account holders of protected accounts with a reporting channel that is available at all times for the purposes of reporting unauthorised or erroneous transactions, and blocking further access via mobile and online channels to his protected account.

4.20 The reporting channel should have all the following characteristics.

(a) The reporting channel[14] may be a manned phone line, phone number to which text messages can be sent, online portal to which text messages can be sent, a monitored email address, mobile application of the responsible FI, or the ATMs of the responsible FI.

(b) Any person who makes a report through the reporting channel should receive a written acknowledgement of his report through SMS, email, or in-app notification.

(c) The responsible FI should not charge a fee to any person who makes a report through the reporting channel for the report or any service to facilitate the report.

Responsible FI to implement real-time detection and blocking of suspected unauthorised transactions

4.21 A responsible FI should have in place capabilities to detect and block suspected unauthorised transactions at all times. A responsible FI should also have capabilities to inquire into the authenticity of the suspected unauthorised transactions before allowing such transactions to be executed. A responsible FI should review the effectiveness of its detection parameters for suspected unauthorised transactions on an annual basis, or as and when there are material triggers.

Responsible FI to assess claims and complete claims investigation

*4.22 A responsible FI should assess any claim made by any account holder in relation to any unauthorised transaction covered in Section 5 ("**relevant claim**") for the purposes of assessing the account holder's liability in accordance with Section 5. It should have a proper governance structure and investigation process, involving representatives who are independent from business units who are to carry out the above assessment.*

4.23 Where the responsible FI has assessed that the relevant claim does not fall within Section 5, the responsible FI should resolve such a claim in a fair and reasonable manner. The responsible FI should communicate the claim resolution process and assessment to the account holder in a timely and transparent manner.

4.24 The responsible FI may require that any account holder furnish a police report in respect of an unauthorised transaction claim, before the responsible FI begins the claims resolution process. In doing so, the responsible FI should, upon request by the account holder, provide information on the procedure to file a police report.

4.25 The responsible FI may request any account holder to provide information set out in paragraph 3.18. Upon enquiry by an account holder, the responsible FI will be expected to provide the account holder with relevant information that the responsible FI has of all the unauthorised transactions which were initiated or executed from a protected account, including transaction dates, transaction timestamps and parties to the transaction.

[14] Account holders may also choose to report unauthorised or erroneous transactions in person at the operating premises of the responsible FI where practicable, subject to their operating hours.

4.26 The responsible FI should complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases. Complex cases may include cases where any party to the unauthorised transaction is resident overseas or where the responsible FI has not received sufficient information from the account holder to complete the investigation. The responsible FI should within these periods give each account holder that the responsible FI has been instructed to send transaction notifications to in accordance with paragraph 3.1 a written or oral report of the investigation outcome and its assessment of the account holder's liability in accordance with Section 5. The responsible FI should seek acknowledgement (which need not be an agreement) from that account holder of the investigation report.

*4.27 Where the account holder does not agree with the responsible FI's assessment of liability, or where the responsible FI's has assessed that the claim falls outside of Section 5, the account holder and the responsible FI may proceed to commence other forms of dispute resolution, including mediation at the Financial Industry Disputes Resolution Centre Ltd ("**FIDReC**") where the responsible FI is a FIDReC member.*

Responsible FI to credit protected account

4.28 The responsible FI should credit the account holder's protected account with the total loss arising from any unauthorised transaction[15] as soon as the responsible FI has completed its investigation and assessed that the account holder is not liable for any loss arising from the unauthorised transaction. The responsible FI should disclose this arrangement to the account holder at the time the account holder reports the unauthorised transaction to the responsible FI, and inform the account holder of the timeline for completing its investigation in accordance with paragraph 4.26.

Scheduled system downtime

4.29 Where relevant, paragraphs 4.2, 4.7, 4.9, 4.10, 4.13, 4.14, 4.19 and 4.21 shall apply during a scheduled system downtime. The responsible FI is to ensure continued delivery of key services and alternatives, where applicable. The responsible FI should also ensure that scheduled system downtime is not performed during periods where high volume of transactions are expected.

Definitions

For the purposes of the E-Payments Guidelines:

*"**access code**" means a password, code or any other arrangement that the account user must keep secret, that may be required to authenticate any payment transaction or account user, and may include any of the following:*

(a) personal identification number, password or code;
(b) internet banking authentication code;
(c) telephone banking authentication code;
(d) code generated by an authentication device;
*(e) code sent by the responsible FI by phone text message such as Short Message Services ("**SMS**"),*

[15] For the avoidance of doubt, losses arising from unauthorised transactions exclude any loss of business or profit, special, punitive, indirect or consequential loss and any other losses

but does not include a number printed on a payment account (e.g. a security number printed on a credit card or debit card);

*"**account agreement**" means the terms and conditions that the responsible FI and account holder have agreed to that governs the use of a payment account issued by the responsible FI to the account holder;*

*"**account contact**" means the contact information that the account holder provided the responsible FI under paragraph 3.1;*

*"**account user**" means—*

(a) any account holder; or

(b) any person who is authorised in a manner in accordance with the account agreement, by the responsible FI and any account holder of a protected account, to initiate, execute or both initiate and execute payment transactions using the protected account;

*"**authentication device**" means any device that is issued by the responsible FI to the account user for the purposes of authenticating any payment transaction initiated from a payment account, including a device that is used to generate, receive or input any access code;*

*"**account holder**" means any person in whose name a payment account has been opened or to whom a payment account has been issued, and includes a joint account holder and a supplementary credit card holder;*

*"**bank"** has the same meaning as in section 2(1) of the Banking Act (Cap. 19);*

*"**currency**" means currency notes and coins which are legal tender in Singapore or a country or territory other than Singapore;*

*"**digital payment token**" has the same meaning given by section 2(1) of the Payment Services Act 2019;*

*"**e-money**" has the same meaning given by section 2(1) of the Payment Services Act 2019;*

*"**finance company**" has the same meaning as in section 2 of the Finance Companies Act (Cap. 108);*

"high-risk activities" include, but are not limited to –

(a) adding of payees to the account holder's payment profile;

(b) increasing the transaction limits for outgoing payment transactions from the payment account;

(c) disabling transaction notifications that the responsible FI will send upon completion of a payment transaction; and

(d) change in the account holder's contact information including mobile number, email address and mailing address.

*"**money**" includes currency and e-money but does not include digital payment tokens;*

*"**non-bank credit card issuer**" means a person who is granted a licence under section 57B of the Banking Act (Cap. 19);*

*"**payment account**" has the same meaning given by section 2(1) of the Payment Services Act 2019;*

*"**payment transaction**" means the placing, transfer or withdrawal of money, whether for the purpose of paying for goods or services or for any other purpose, and regardless of whether the intended*

recipient of the money is entitled to the money, where the placing, transfer or withdrawal of money is initiated through electronic means and where the money is received through electronic means;

*"**protected account**" means any payment account that —*

(a) is held in the name of one or more persons, all of whom are either individuals or sole proprietors;

(b) is capable of having a balance of more than S$1,000 (or equivalent amount expressed in any other currency) at any one time, or is a credit facility;

(c) is capable of being used for electronic payment transactions; and

(d) where issued by a relevant payment service provider is a payment account that stores specified e-money.

*"**relevant exempt payment service provider**" means any exempt payment service provider under section 13(1)(a) to (d) of the Payment Services Act 2019 that provides account issuance services where each payment account issued stores e-money;*

*"**relevant payment service provider**" means any major payment institution as defined in section 2(1) of the Payment Services Act 2019 that has in force a licence that entitles it to carry on a business of providing account issuance services or any relevant exempt payment service provider;*

*"**responsible FI**" in relation to any protected account, means any bank, non-bank credit card issuer, finance company or relevant payment service provider that issued the protected account;*

*"**sole proprietor**" means any business owned by an individual where the owner is personally liable for debts and losses of the business;*

*"**specified e-money**" has the same meaning given by section 2(1) of the Payment Services Act 2019;*

*"**transaction notification threshold**" means –*

(a) the threshold for transaction alerts set by the account holder; or

(b) if the account holder did not set any threshold for transaction alerts, the default industry-baseline transaction notification threshold.

*"**unique identifier**" means a combination of letters, numbers or symbols specified by the responsible FI to the account holder and is to be provided by the account user in relation to a payment transaction in order to identify unambiguously one or both of —*

(a) any person who is a party to the payment transaction;

(b) any person's payment account;

*"**unauthorised transaction**[16]" in relation to any protected account, means any payment transaction initiated by any person without the actual or imputed knowledge and implied or express consent of an account user of the protected account. This includes "seemingly authorised transactions" as defined in the Guidelines to the Shared Responsibility Framework.*

[16] *The following are examples of payment transactions that do not fall within the scope of unauthorised transactions:*

(a) The account user knew of and intended to make the payment transaction, notwithstanding that the transaction could have arisen as a result of falling victim to a scam (e.g., e-commerce, government- official impersonation, job, investment or love scams);

(b) The transaction was performed by a person as a result of the account holder sharing access and usage of their devices with the person, or storing the person's biometrics identities on their devices. The account holder is deemed to have consented to the use of his account by this person.