APPENDIX H
(To Merchant Services Terms and Conditions)
Applicable to QR Code Transactions

1. ADDITIONAL UNDERTAKINGS/PROVISIONS RELATING TO QR CODE TRANSACTIONS

For QR Code Transactions:-

(a) The Merchant must only use the QR Code (Static) to collect monies for its own sales and not share or duplicate the QR Code (Static) for use by any other third party. If the Merchant believes that their QR Code (Static) has been tampered with or damaged, the Merchant must immediately notify the Bank to reprint and replace the same.

(b) The Merchant must not generate any QR Code (Dynamic) at any location which exceeds a certain distance (*as prescribed by the Bank*) from the Merchant's outlet address ("**Unauthorised Location**"). The devices used by the Merchant to generate QR Code (Dynamic) are installed with an anti-fraud geo location feature. If a QR Code (Dynamic) is generated at any Unauthorised Location, a fraud alert will be triggered.

(c) Where a Merchant only carries out QR Code Transaction using a QR Code (Static) and does not use any other Payment Channels:-

(i) a report of QR Code Transactions carried out for each day will be provided to the Merchant by the next Business Day. The Merchant will receive a notification when the report is ready for review and the Merchant shall log into the CIMB Merchant Electronic Online Portal (e-Access) to review said report;

(ii) the Bank shall pay the settlement fund due to the Merchant within (i) one (1) Business Day following the QR Code Transaction performed before 8p.m., and (ii) two (2) Business Days for QR Code Transaction performed after 8p.m. unless the Bank receives notice from the Card Companies, PayNet and/or eWallet Operators requiring the Bank to withhold payment to the Merchant;

(iii) if the Bank does not receive the settlement fund from the eWallet Operator, the Bank and the Merchant shall agree to defer the Bank's payment to a date to be mutually agreed between the Bank and subject to these terms and provisions. Any discrepancies or errors arising from the settlement process, must be notified to the Bank in writing within seven (7) Calendar Days from the date of the Bank's payment, failing which the Merchant shall be deemed to have waived its right to make any claim against the Bank in respect of such discrepancies or errors;

(iv) if any dispute between the Cardholder / eWallet Users and the Merchant arise in the course of a QR Code Transaction using a QR Code (Static), the process used to resolve the disagreement between the Cardholder / eWallet Users and the Merchant shall be based on the rules prescribed by the Card Companies, PayNet or the operator of the platform upon which the QR Code Transaction was carried out and in the absence of any such rules, the Merchant shall solely be responsible for resolving the dispute amicably with the Cardholder / eWallet Users without involving the Bank.

(d) The Merchant and their Sales Reps shall observe all security measures prescribed by the Bank from time to time relating to QR Code Transactions.

(e) The Merchant shall comply with all procedures as communicated by the Bank to the Merchant from time to time, which are necessary to prevent and mitigate potential risks (such as fraud and settlement risks).

(f) The Merchant shall bear the risks of loss where there is:

(i) interception of transactions which may result in transactions being made to an unintended and unauthorised third party;

(ii) any unauthorised transactions where the security of the transaction has been compromised;

(iii) any unauthorised manipulation of any QR Code;

(iv) tampering of the displayed QR Code (Static) which may result in payment to an unintended third party other than the Merchant; and/or

(v) delay and/or failure in payments being effected to the Merchant and/or failure of transactions due to:

1. technical error, malfunction or omission on the part of the Bank, Card Companies, PayNet and/or eWallet Operators;
2. maintenance activity being conducted in respect of the relevant system infrastructure;
3. telecommunications network congestions, network failure, systems failure or any other reason beyond the reasonable control of the Bank;
4. an unauthorised person or third party having accessed the Merchant's Terminal or any other related computer or electronic systems; and/or
5. any data loss or theft due to any virus or malware.

2. APPENDIX H IS TO BE READ WITH MERCHANT SERVICE TERMS AND CONDITIONS

This Appendix H is to be read together with the Bank's Merchant Services Terms and Conditions. If other Payment Channels are being used by the Merchant, the respective terms and conditions governing those Payment Channels shall also apply if QR Codes are used in conjunction with those Payment Channels. Where there is inconsistency, Appendix H shall override the Merchant Services Terms and Conditions.

● The remaining page is intentionally left blank ●