Cards Payment Gateway

1. What are the Benefits of Cards Payment Gateway?

I. The largest base of credit and debit cardholders available to merchants participating in the marketing programmes
II. You can view the transaction record on the Maybank eBPG Portal real time
III. Helpdesk / Merchant service hotline and technical support team
IV. 24-hour authorisation service for customers

2. What are requirements to apply Card Payment Gateway?

I. The company must be locally registered in Malaysia.
II. The company must have a Maybank business current account.
III. The company must have an appropriate office site and should not be operating from personal home/residential area.
IV. The website must be ready and comply with Maybank's website checklist requirements as below:

a) Minimal Website Requirement

- The website must be ready for publishing or being develop
- The website must use at least 128-bit Secure Socket Layer (SSL) encryption technique or protocol
- The website must belong to the registered company which submit this application to Maybank
- Accepting only 3D secure transaction

b) Merchant Information

- Merchant must clearly display information about the company and address on the website
- Merchant is not allowed to share the eBPG facilities with other company or sub-merchant

c) Product Information

- The website must clearly indicate details of your products and services
- Merchant must clearly display the total cost (including the cost of delivery, handling and applicable taxes of your products and services) on the website

d) Payment Information & Security

- Merchant must clearly display the currency type on the website
- Merchant must provide an online invoice/receipt to customer upon completion of any card's transaction via the website which contains the following:

- Merchant's trading name

- Merchant's website (URL)

- Transaction amount

- Currency Type

- Transaction Date

- Cardholder's Name

- Authorization Code

- Description of Products and Services

- Return / Refund Policy

- Merchant must send a confirmation e-mail to customers upon the successful purchase of products and services
- Merchant must make sure that the name (Trading name) and country that appear on the cardholder's statement easily recognizable to the cardholder as stated on the website.If merchant transacts on behalf of customers by storing their credit card details into the payment server, merchant must present a PCI-DSS to Maybank.

e) Delivery / Shipping

- Merchant must display a clear Terms & Condition and/or refund policy on the website (e.g. method of return, days of refund, etc)
- The customers have to expressly accept the merchant's Terms & Conditions (e.g. online transactions, return policy, etc) before completing the transaction
- Merchant must display a clear delivery/shipping method on the website (e.g. courier, parcel locker, COD)
- Merchant must provide estimated time of delivery/shipping to customer
- Merchant must provide a delivery/shipping tracking reference number to customer

f) Support

- Merchant must clearly display customer service details on the website (e.g. phone number with country code or e-mail address)
- Merchant must store customer profiles on the website for support purpose

- Merchant needs to develop or set-up own merchant’s web server at merchant own cost for the integration with Maybank eBPG.
- Merchant must have fraud mitigation policy and/or system that can mitigate the online credit card fraud risks. If Merchant used any of the anti-fraud warning system software/application, the system must at least but not have limited to the following features:

a) Web site security

We strongly suggest that merchant's e-commerce web site is equipped with security facilities like SSL, encryption and firewall. This way, the merchant's database (especially the sensitive sales information) and its transmission are safe from being accessed by outsiders.

b) Order details

Merchants should urge customers to provide adequate information upon ordering, especially contact information of the customers. Make sure that the customer is a legitimate cardholder. More attention is required for suspicious orders (like remote delivery addresses or simultaneous multiple orders).

c) Freemail address

Some fraudsters attempt to mask their identity by using a freemail address. While most users of freemail addresses are indeed legitimate, caution should be exercised for orders with freemail addresses, especially when this is the only way to contact the customers.

d) Out-of-norm

Merchant should be wary of orders that falls outside usual ordering patterns, like bulk orders or purchases that greatly exceed the average transaction amount.

e) IP record

Beware of orders made from odd locations (which are sometimes traceable with the IP addresses), especially where credit card fraud is more common.

f) Proof delivery

Get a signed proof of delivery or receipt if available upon retrieval request.

g) Return

Merchants should devise and maintain clear, easy to understand and consistent product return policies to keep customers well informed

3. What are the types of cards can Cards Payment Gateway accept?

Cards Payment Gateway accepts VISA, Mastercard and American Express Cards

4. What are the fees that I have to pay?

The Merchant Rate, setup fee (if applicable) and annual maintenance fee (if applicable) will be provided in the Letter of Offer upon application approved.

5. Is there any testing required after Maybank eBPG integration is completed?

Yes, a testing is required once the integration process is completed. This test will take about three (3) days and you may extend the testing date provided you have obtained confirmation from the bank. You are given six (6) months to complete the integration and testing with Maybank eBPG, failing which the offer will lapse

6. What is the notification period before going Live?

Once the testing is successful, you can request to be in the live environment. You are required to notify the bank 3 (three) days in advance.

Are there any "best practices" guidelines for E-Commerce Merchants?

I. Understand the risk of E-Commerce environment.

Merchant needs to understand the risks of selling over the Internet as the purchaser may not be the genuine cardholder.

II. To maintain high customer satisfaction to avoid any customer disputes. For example:

a) Goods and services are described accurately on your websites.
b) Notify cardholder of any delays.
c) Deliver merchandise on a timely basis and advised customers when they can expect it.

III. Recommended internal merchants fraud prevention system:

a) Required transaction data fields

Required transaction data fields in website that can help to identify risk and require the customer to complete them. This information will help merchant to assess the fraud risk of a transaction. Edit and validate required data field in real time. Key risk data fields include:

- Demographic information such as telephone numbers, that can be validated using telephone directory and to verify the transaction with the customers.
- E-mail address, particularly when it involves an 'anonymous' service.
- Cardholder name and billing address can be validated using directory.
- Shipping name and address, particularly if this information is different from the cardholder's billing information.

b) Cardholder validation by:

- Check the validity of the customer's telephone number, physical address and e-mail address.
- Screen for high-risk international addresses.
- Test the validity of the e-mail address by sending an order confirmation message
- Establish effective procedure for cardholder verification calls.

C) Tracking and analysis activity at merchant in monitoring the patterns of risk exposures. Examples:

- Track the Web addresses or IP addresses that are used to reach merchant websites.
- Collect and analyze Internet customers 'click through' patterns for fraud risk screening.
- Track purchase patterns of registered customers.
- Track multiple order decline rates based on card number, customer IP address, etc.

d) Establish fraud screening / monitoring transactions.

- Establish individual cardholder limits based on the number and amount of transactions that have been approved within a specified number of days. It enables adjustment of limits according to customer purchase patterns.
- Establish limits for single transaction amounts and consecutive repeat sales.
- Ensure the velocity limits are check against multiple characteristics including billing address, shipping address, telephone numbers and e-mail address.
- Check records to see whether the same delivery address has been used before with different card details.
- Contact the cardholders who exceed review limits to determine transaction activity is legitimate.

iv. Data Security

Conduct annual review of systems control.

v. Transaction handling / storing:

a. Storing of minimal information for card-not-present environment:

- The name as appears on the card
- A customer contact phone number. Always ask for a permanent number.

b. Merchant may store the transaction information for record purposes

c. Merchant needs to ensure customer information is destroyed when it is no longer needed.

vi. Remarks

All the above E-Commerce best practices are guidelines for E-Commerce merchants to ensure the integrity of payment services provided to customers. You may conduct additional practices in mitigating disputes and fraudulent transactions at their establishment

7. How will my funds be deposited?

For all settled transactions, your funds will be deposited into your current account on the next business day

8. Where can I view the transaction records?

You can view this on the Maybank eBPG Portal. You will be provided with an account and login credentials.

9. Where can I view the settlement reports?

You can view this on the e-statement Merchant Portal. You will be provided with an account and login credentials.

10. Who can I contact for inquiry and clarification?

For further assistance or clarification, you may email to merchantinquiry@maybank.com