MAYBANK E-COMMERCE CREDIT CARD FACILITY
Online Credit Card Payment

By : E-COMMERCE
MERCHANT BUSINESS
CARDS BUSINESS GROUP
MAYBANK
38TH Floor Menara Maybank
100 Jalan Tun Perak
50050 Kuala Lumpur

Version : 3.3

Updated : 1st October 2011
Maybank e-Commerce Credit Card Facility is offering two (2) types of payment services for merchants to accept online credit card payment via Internet. The payment services are known as Maybankard.net and Maybank2u.com. These e-services are hosted at Maybank and have a built-in interface to integrate with merchant’s website and store front server to enable online credit card payment under a 3DSSL protocol.

1.0 Maybankard.net

Maybankard.net is a real-time transaction processing system that functions as a payment gateway switch using a secure transaction server on the Internet. Merchants with a valid, enabled merchant account can use the system to submit, authorize and capture card transactions. In addition to the normal e-commerce functionality, Maybankard.net supports 3-D Secure transactions, web-service based transactions and several other mechanisms, utilities and applications to help you process and manage e-commerce transactions.

To offer a complete e-commerce authorization system, Maybankard.net is made up of three main modules: the Checkout Application, the Merchant Plug-In and the Merchant Administration. The Checkout Application is the main module for e-commerce transaction processing. The Merchant Plug-In, or MPI for short, is the module that is fully integrated with the Checkout Application and is responsible for handling the 3-D Secure protocol. TheMerchant Administration is the main front end application that provides a user friendly interface that can be used to manage your transactions.
2.0 Maybank2u.com

Maybank2u.com is a strategic alliance that gives merchants the opportunity to sell merchant’s products and collect payments from your customers online.

**In order for merchants to have the credit card payment facilities in Maybank2u.com, merchants must have or registered their company as Maybank2u debit payment facilities.

Merchant’s customers can make payments via:

- **Maybank2u.com**
  Maybank2u.com is a financial portal that provides information and online financial services comprising of online banking, online stocks, online insurance, online shopping and bill payment services. Merchant’s customers can pay their bills online by debiting their Maybank Savings/Current Account(s) or Credit Cards issued locally by Maybank and other financial institutions.

- **Merchant Website (Payment Link/Debit Engine)**
  With Maybank2u.com payment link deployed at merchant’s website, merchant’s customers can make payments online at merchant’s website by debiting their Maybank Savings/Current Account(s) or Credit Cards issued locally by Maybank and other financial institutions.

To ensure safety and confidentiality of transactions, all payments are done in a secured environment. We have employed the latest Internet security technology and various security practices in our portal.
3.0 MAYBANK E-COMMERCE CREDIT CARD FACILITY MERCHANT’s REQUIREMENT

Minimum Requirements

1. To be a Public Listed/Sdn Bhd company.
2. Number of years in the business must be at least 1 year in operation.
3. The company must have an appropriate office site and should not be operating from personal home / residential area.
4. The company must be locally registered in Malaysia.
5. Minimum monthly sales of **RM50,000.00**
6. The website must be ready and comply with Maybank’s website checklist requirements as per **Appendix II**.
7. Merchant needs to install (coding) MPI at merchant’s web server at merchant own cost for the integration with Maybankard.net and Maybank2u.com.
8. Merchant must have a fraud mitigation system that can mitigate the credit card fraud online. If Merchant used any anti-fraud warning system software/application, the software must at least have the following features:-
   i. Fraud behaviour detection
   ii. Black list check
   iii. Risk ranking indicator
   iv. Multiple attempt indication

Documents

The e-Commerce Merchant Application Form must also be accompanied by certified true copies of the following documents:-

i. Form 49
ii. Form 24
iii. M & A
iv. Company Profile (Hard Copy - in addition to the web site)
v. Company Current A/C or Bank Statement for the last 6 months.
vi. If the company does not have MBB Current A/C, please furnish us the copy from other banks/financial statements for the last 6 months.
vii. Company’s Resolution or Board of Director’s Resolution for authorised signatory to operate current account.
viii. Proposal on Business Model
ix. Financial Statement / Audited P&L (last 2 financial years)

Forwarding Address

You need to fill in the application form on **Appendix I** and submit all the necessary documents as stated above to the following address :-

<table>
<thead>
<tr>
<th>e-Commerce</th>
<th>Maybank2u.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Business Department</td>
<td>Business Planning &amp; Development Department, eChannels, Retail Financial Services, Malayan Banking Berhad,</td>
</tr>
<tr>
<td>Card Business Group</td>
<td>23rd Floor, East Wing Menara Maybank,</td>
</tr>
<tr>
<td>Malayan Banking Berhad</td>
<td>100, Jalan Tun Perak,</td>
</tr>
<tr>
<td>38th Floor, Menara Maybank</td>
<td>50050 Kuala Lumpur,</td>
</tr>
<tr>
<td>100, Jalan Tun Perak</td>
<td>50050 Kuala Lumpur,</td>
</tr>
<tr>
<td>50050 Kuala Lumpur</td>
<td></td>
</tr>
</tbody>
</table>
Merchant Discount Rate
Upon reimbursement to the company’s current account, each transaction is deducted based on the MDR offered by the bank. Indicatively, the range of MDR is between 3.0% to 5.0% or higher (subject to Maybank’s recommendation).

Pricing/Fee

<table>
<thead>
<tr>
<th></th>
<th>Maybankard.net</th>
<th>Maybank2u.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Transaction Fee</td>
<td>Merchant Discount Rate (MDR)</td>
<td>Merchant Discount Rate (MDR) - credit card</td>
</tr>
<tr>
<td>2. Processing fee</td>
<td>RM100-00</td>
<td>RM100-00</td>
</tr>
<tr>
<td>3. Stamping fee</td>
<td>RM20-00</td>
<td>RM20-00</td>
</tr>
<tr>
<td>4. Integration fee</td>
<td>By own or third party IT provider</td>
<td>By own or third party IT provider</td>
</tr>
<tr>
<td>5. Other Fee</td>
<td>RM2000 Annually</td>
<td>Must have debit payment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One Time RM2000 for debit facilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service Charge of MDR/transaction fee or minimum of RM100 whichever is higher.</td>
</tr>
</tbody>
</table>

Currency
Currently, Maybank offers 2 types of currencies which are Malaysian Ringgit (MYR) and US Dollar (USD). For this matter, please specify the currency that you wish to have. However, settlement to merchant will be in Malaysian Ringgit (MYR). Maybank2u offers only for local credit and settlement in Malaysia Ringgit (MYR).

Approval Time Frame
Upon receipt of your application form and other documents from your company, the application will be processed within 2 or 3 weeks. During this period, we may call you for further enquiries or make a site visit.

Approved Documents
Once application is processed and approved, we shall furnish you with the following documents:-
- 2 sets of e-commerce credit Card Acceptance facility letter of Offer
- 2 sets e-commerce Merchant Agreement

Notes:
1. The letter and agreement must be signed by Authorised Signatory of the company. Stamping of agreement will be made by the bank and a copy of this stamped agreement shall be forwarded to you.
2. Upon approval, merchants are given Six (6) month from the date of the Letter Offer/Agreement to complete the Integration work with Maybank’s Payment Gateway, failing which the offer will lapse and merchant is required to submit a new application.

MPI Installation
Merchant needs to install (coding) MPI at merchant’s web server at merchant own cost for the integration with Maybankard.net and Maybank2u.com.

Testing
Once integration process is completed, you can request for a testing date from Maybank. The merchant should inform Maybank three (3) days before the testing date. This test will take about three (3) days and you may extend the testing date provided you had obtained confirmation from the bank.

Live Cut-Over
Once the testing is successful, you can request to be in the live environment. Please notify us at least 3 (three) days in advance.
4.0 FAQ

What is the Maybank e-Commerce Credit Card Facility?
Maybank e-Commerce Credit Card Facility covers the range of on-line business activities for products and services, both business-to-business and business-to-consumer, through the Internet. It offers a comprehensive e-Commerce Acquiring payment of enabling businesses to realize e-commerce transactions by providing a user-friendly, yet secure on-line payment acceptance platform on the Internet.

Who can apply for Maybank e-Commerce Credit Card Facility?
We accept applications from any businesses, organizations and charitable bodies registered in Malaysia. Please refer to our Maybank e-Commerce Merchant Requirement.

What is the Maybankard.net?
Maybankard.net is a comprehensive e-Commerce acquiring payment authentication services, which is Visa and MasterCard compliant to its cardholders and merchants.

What are the key features of the Maybankard.net?
We offer a payment acceptance solution to process multi-currency transactions such as Australia, Britain, Japan, Hong Kong, Europe, Singapore, USA and Thailand. Apart from the comprehensive ranges of tools on user administration, reverse and refund and transaction reporting, we provide the value added processing and security features of 3D security protection.

What payment cards can Maybankard.net accept?
Maybankard.net accepts Visa, MasterCard and American Express card payments.

In what currency does Maybank e-Commerce Credit card merchant would receive in their settlement payment?
Maybank e-Commerce merchants will receive the settlement payment as per transacted currency and it will be auto credited into your Foreign Currency Account. However multi-currency transactions only apply to Foreign Credit Cards.

What are the charges for Maybank e-Commerce Credit card Facility payment acceptance?
Merchants will need to pay a one-off set up charge, an annual service charge for Maybankard.net and transaction commissions based on the payments received.

Do I need to install a shopping cart in my web site?
We strongly recommend that, in order to operate e-commerce activities, web sites should have online catalogues that front their payment facilities, which are known as shopping carts. Our payment services require installation of a shopping cart on the merchant’s side. You have to liaise with IT vendor or Internet Service Provider that provide the shopping cart facilities software.

Do I need to have a web site before we can apply for your services?
Yes, in order to implement the services, merchant has to own and run a web site. However, during the application period you are not required to have a running web site. You may want to contact us when your site is ready for publishing or you may choose to apply for our services while your site is being develop.

Can I become your merchant without a web site?
No. For Maybankard.net, merchants must have their own web sites.
I am running the online operations outside Malaysia. May I join?
Currently we provide payment acceptance services to all businesses, organizations and charitable bodies registered in Malaysia only.

What documents are required in order to apply for your payment acceptance services?
Please refer to our Maybank e-Commerce Credit Card Facility Merchant's Requirement.

My company operates more than one e-commerce site. Do I have to apply for multiple merchant accounts?
Yes, merchant id is offered for use at only ONE web site. Merchants should apply for separate ids for each of the sites they operate.

What is 3D SSL?
3D SSL is the new safety requirement to carry out your purchases on line. 3D SSL is based on the new technology implemented by Visa known as “Verified by Visa”, MasterCard known as “MasterCard SecureCode” and American Express known as “American Express Safekey”. This service objective is to ensure that only the cardholder can make online purchases via the Internet using his/her credit card.

What exactly are “Verified by VISA”, “MasterCard SecureCode” and “American Express Safekey”?
"Verified by Visa”, “MasterCard SecureCode” and “American Express Safekey” is a program designed to provide online retailers the added security of having Issuing banks authenticate their individual cardholders and qualify their online transactions for protection against “cardholder unauthorized” or "I didn't do it" chargeback.

What is a chargeback?
A chargeback is the forced reversal of a transaction by the credit card issuing bank. Chargeback take place when we receive notification from the cardholder's card issuing bank that has received a dispute notice from the cardholder, whose card had been charged by our merchants. In certain cases defence is possible (e.g. order denial while delivery is completed indeed), given merchants are able to provide adequate evidence. Sometimes (for example, fraudulent card usage) a chargeback is made immediately. Please note that excessive chargeback may result in service terms revision, service suspension or even termination.

How does “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” work?
When a cardholder is on your check-out page, the “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” service performs the following to ensure that the cardholder is authorized to make this transaction:
1. It initiates a pop-up box into which the cardholder enters a private code that is registered with the bank that issued the card.
2. It passes the authentication value in your normal authorization request procedures and, if approved, receives an authorization that binds that customer to that transaction. This authentication value is transported with an ECI value.

“Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” is neither the first nor the only method of security being promoted to me by card companies. Why should I adopt this one?
“Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” is the result of several years of learning by Visa, MasterCard and American Express from past secure online payment services and is focused on making the process easy for merchants and cardholders while addressing your concerns. “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” uses a similar concept and similar business rules to that which is already used in bricks and mortar businesses. Most importantly, it protects your business from fraudulent transactions and disputes, enabling you to grow more profitably.
I already use SSL, why is “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” better?
“Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” also uses SSL, but adds the important security function of confirming the identity of the Visa, MasterCard or American Express cardholder, creating a virtual “card present” environment. It is this important additional function that enables Card Issuers to provide your business with guaranteed payment.

You need to integrate Merchant Plug-In with your existing server, or your IT service provider may be able to do this on your behalf. There are no required changes to the customer-facing portion of your e-commerce application.

How much time will it take to implement “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey”?  
On average, it takes 3-5 man days for integration of the Merchant Plug-In with your legacy system. Maybank may provide assistance with this process.

How will cardholders know that I have “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey”?  
A “Verified by Visa”, “MasterCard SecureCode”, “American Express Safekey” logo or participation mark must be featured on your web site.

Once it is installed, what do I have to do?  
You can now proceed to accept Visa, MasterCard and American Express as a means of payment via your website.

How much maintenance is required for the Merchant Plug-In?  
Like any software, the Merchant Plug-In may experience problems that require troubleshooting and upgrades may be available from time to time. Maybank will supply for these circumstances.

How much longer does a “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” transaction take?  
On average, the “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” process adds 10-20 seconds to the total transaction time.

How do I recognize a “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” registered card?  
The Merchant Plug-In automates this process for you by checking with the Card Issuer to see if the card is registered and then automating the process for authentication.

How do I treat cards that are not registered for “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey”?  
Process card transactions that don't have “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” with the same precautions that you currently use, understanding that these transactions do not carry the same benefits of guaranteed payment as a “Verified by Visa”, “MasterCard SecureCode” or “American Express Safekey” transaction.

I'm concerned with the issue of online fraud. What should I do to minimize fraud?  
Fraudulent behaviour online takes various forms from stolen card to system hacking. We would like to suggest the following actions to minimize fraud.

- **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.

- **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).

- **Freemail address**
  Some fraudsters attempt to mask their identity by using a freemail addresses. 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.

- **Out-of-norm**
  Merchants should be wary of orders that falls outside usual ordering patterns, like bulk orders or purchases that greatly exceed the average transaction amount.

- **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.

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

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

For Maybank2u FAQ, please refer to [www.maybank2u.com](http://www.maybank2u.com)
MERCHANT APPLICATION FORM
Facilities Required:
Visa/MasterCard:

<table>
<thead>
<tr>
<th>Point Of Sales</th>
<th>Mail Order</th>
<th>Telephone Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autopay</td>
<td>eCommerce</td>
<td>M2U</td>
</tr>
</tbody>
</table>

American Express:

<table>
<thead>
<tr>
<th>Point Of Sales</th>
<th>Mail / Telephone Order</th>
<th>Autopay</th>
</tr>
</thead>
<tbody>
<tr>
<td>eCommerce</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Others:

<table>
<thead>
<tr>
<th>EzyPay</th>
<th>eDebit</th>
<th>Union Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCB</td>
<td>DCC</td>
<td></td>
</tr>
</tbody>
</table>

Merchant Details:

Trading Name: ________________________________

Register Name: _______________________________

Trading Address: ____________________________________________________________

_________________________________________________________________________

Head Quarter Address: ______________________________________________________

_________________________________________________________________________

Nature of business: _________________________________________________________

Contact Person : ________________________ Contact Number: _______________________

Email address: _____________________________________________________________
## WEBSITE COMPLIANCE

### Secured Internet Site declaration (as applicable)

<table>
<thead>
<tr>
<th>No</th>
<th>Item</th>
<th>Compliance by Merchant (Y,N,N/A)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Is the Merchant's identity and location clearly indicated?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>2</td>
<td>Are the products and services offered clearly indicated?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>3</td>
<td>Are the total costs, including shipping, handling and applicable taxes, clear to the cardholder?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>4</td>
<td>Is the transaction currency clearly indicated?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>5</td>
<td>Are the Merchant's shipping practices clearly indicated?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>6</td>
<td>Can the cardholder determine when to expect the merchandise?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>7</td>
<td>Is the Merchant's return policy easily accessible and understandable?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>8</td>
<td>Does the cardholder have to expressly accept the Merchant's return policy before completing the transaction?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>9</td>
<td>Is a customer service phone number or e-mail address clearly available for cardholder to resolve disputes (and do phone numbers include a country code)?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>10</td>
<td>Are the <em>Cardholder’s Name, Billing Address and Phone Number</em> clearly available for merchant to resolve disputes?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>11</td>
<td>Does the Merchant confirm the sale via e-mail after the order has been placed?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>12</td>
<td>Does the Merchant keep the cardholder notified of the shipping status of ordered goods?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>13</td>
<td>Are the name and country that will appear on the cardholder’s statement easily recognizable to the cardholder as that on the website?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
<tr>
<td>14</td>
<td>Does the Merchant provide gambling facility to the cardholder?</td>
<td>N= OK</td>
<td>Y= Have to comply</td>
</tr>
<tr>
<td>15</td>
<td>Does the Merchant operate the business at the proper office and not at the residential?</td>
<td>Y= OK</td>
<td>N= Have to comply</td>
</tr>
</tbody>
</table>

*NOTE: Please provide a copy of the e-mail*
<table>
<thead>
<tr>
<th>No</th>
<th>Item</th>
<th>Compliance by Merchant (Y,N,N/A)</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 16 | Does the Merchant transact on behalf of the cardholder by keeping in cardholder’s credit card details into the payment server? | N= OK  
Y= Have to comply | |
| 17 | Does the Merchant’s web site belong to the registered company which has been recruited by Maybank? | N= Have to comply | |
| 18 | Does the Merchant allow any another company share its Maybank e-Commerce Credit Card Acceptance Facility or Maybank2u Credit Card Payment Portal Facility to operate as Master merchant to the sub-Merchant? | N= OK  
Y= Have to comply | |
| 19 | Does the Merchant use at least 128-bit Secure Socket Layer (SSL) encryption technique or protocol for the transmission of cardholder’s information? | Y= OK  
N= Have to comply | |
| 20 | Does the Merchant’s website capable of accepting and transmitting the CVV2 and CVC2 field to Maybank? | Y= OK  
N= Have to comply | |
| 21 | Upon completion of any card’s transaction, does Merchant provide the cardholder with the transaction receipt via the Merchant’s web site? | Y= OK  
N= Have to comply | |
| 22 | Does the transaction receipt contains the following :  
1) Merchant’s Name  
2) Merchant’s on-line address  
3) Transaction amount  
4) Transaction currency in RM  
5) Transaction date  
6) Cardholder’s name  
7) Authorisation code  
8) Description of goods / services  
9) Return/Refund Policy | Y= OK  
N= Have to comply |  
**NOTE:** Please provide a copy of the receipt |
| 23 | Bank Negara’s Requirement :  
1) Take adequate measure to safeguard confidentiality and security of card information.  
2) Use a website at least 128-bit Secure Socket layer encryption technique for transmission of cardholder information. | Y= OK  
N= Have to comply | |
| 24 | Visa’s requirement to enrol in Visa’s Account Information Security (AIS) Programme | N/A | To be enrolled if applicable |
| 25 | MasterCard’s requirement to enrol in MasterCard’s Site Data Protection (SDP) Programme | N/A | To be enrolled if applicable |

**Note :**  
i) Y = Yes  
N = No (These includes sites that cannot be accessed due to broken links, sites that we’re unable to proceed with as they requires registration and credit card details to complete purchase)  
N/A = Not Applicable  
ii) If any of the above requirements are not applicable due to the nature of your business, please specify the reason in your reply letter to us.