Annex A to the Terms and Conditions

E-Commerce/Moto Merchants Supplemental Terms As per Card Scheme Rules

Merchant Website Requirements

Website content requirements are important to ensure a satisfactory shopping experience for customers and to minimize Cardholder copy requests, disputes and chargebacks.

The Merchant's terms and conditions must be available to customers through a clearly visible link on the home page and must cover all of the following:

- Description of Merchant's billing practices. The Merchant must not bill the Cardholder until the merchandise is ready for shipping or the service is completed.

- Return, refund and cancellation policy. A Merchant must indicate its return, refund, and cancellation policy clearly to inform Cardholders of their rights and responsibilities, for example, in case they need to return goods. If the Merchant has a limited or no refund policy, this must be very clearly communicated to Cardholders before the purchase decision is made to prevent misunderstandings and disputes.

- Delivery policy. Not all Merchants are able to support delivery of goods worldwide and may instead restrict sales to within their own country or to a limited number of countries, based on delivery experience or import and export regulations.

  Because Merchants may sustain a loss when shipped goods fail to arrive, they are entitled to establish their own policies regarding the delivery of goods. However, when a Merchant does have restrictions or other special conditions in place, those special conditions must be clearly stated on its website.

- A clear, concise statement of the Merchant's privacy policy regarding the storage and any subsequent use of customer details.

- A description of the site's information security practices.

- Export restrictions (if known).

The web site is also to include:

- Merchants' address information and country of domicile.

- Identifiers that easily match the website to the doing-business-as name.

- Complete description of goods or services. The Merchant must provide a complete description of its goods or services, paying particular attention to whether they are legal or viable outside the Merchant's own country. For example, if selling electrical goods, the Merchant must state voltage requirements, which vary around the world. All additional expenses to be incurred by the Cardholder must be explicitly stated e.g. taxes, packaging or delivery.

- Customer service contact information, including electronic mail address or telephone number.

Since communication with a Merchant is not always possible using the Merchant Website, Merchant must display a customer service contact telephone number or e-mail address. This enables Cardholders to contact the Merchant to ask questions about their Transaction, which in many cases, can avoid the dispute process.

The Merchant Establishment VAT number must be displayed along with the customer service contact information.

- Transaction currency, or currencies and amount.

Since the electronic commerce Merchant's customer base is worldwide, it is important that the Cardholder is made aware of the Transaction currency before the Cardholder proceeds with a purchase. The currency must be clearly stated, including the country name when the name of the unit of currency is not unique. For example, a dollar can be an Australian dollar, a New Zealand dollar, a Hong Kong dollar, a U.S. dollar, or one of many more.

Merchants can display equivalents of the Transaction amount in different currencies, but they must clearly indicate that the equivalents listed are for information only.

- A clear display of Recurring Transaction disclosure statement (where applicable).

- A declaration stating that the site does not constitute an invitation to buy or the solicitation of an offer to sell products or services in any jurisdiction to any person to whom it is unlawful to make such an offer or solicitation in such jurisdiction.

Merchant Transaction Receipt Requirements

Merchants need to be aware of the following unique data requirements for Transaction Receipts and copy fulfillments for electronic commerce Transactions:

- Concealed Cardholder account number. For electronic commerce Transactions, the complete Cardholder account number must not appear on the Transaction Receipt. This minimises the potential for fraud, particularly where the original Transaction, or the Merchant's confirmation, are not encrypted.

- Unique Transaction number. This is an identification number that uniquely identifies the Transaction in question, and assists both the Cardholder and Merchant in tracking orders and in resolving any disputes.

- Merchant online address. The Merchant must always include its website address to help the Cardholder to recognise the Transaction and to contact the Merchant if there are any queries.

In addition, it is suggested that the Transaction Receipt includes wording to indicate that the Cardholder should print, or save, the receipt for his records.

The Merchant can choose to send either a separate e-mail message to the Cardholder containing this required information, or, as with mail and telephone order Transactions, a physical Transaction Receipt in

the mail, or both. To minimize Cardholder enquiries, Merchants are encouraged to send an online acknowledgment of the Transaction in addition to the Transaction Receipt.

Best practices

Additional website features and practices that are highly recommended include:

- Adoption of CVV2/CVC2 code to verify the Cards' authenticity. (For information security purposes, storage of CVV2/CVC2 is strictly prohibited).

- Controls to avoid duplicate Transactions.

- Commitment to process orders promptly. The Merchant should ideally send an e-mail confirmation and order summary within one business day of the initial order. The Merchant should provide up-to- date stock information if item is back-ordered.

- Commitment to respond to all customer service e-mails and phone calls within two business days.

- A statement encouraging Cardholders to print out and retain a copy of the Transaction record.

- Highlighted mandatory fields in the payment form.

- Payment form should request Cardholder's full name on Card and Cardholder's billing and delivery address.

- Card type tick box (e.g. Visa, MasterCard etc.), and matching of Card number with selected card type

- Register with a privacy organization and post a seal of approval on the website.

- Establish Transaction controls and velocity limits and implementation of fraud screening tools to identify high risk Transactions

- Validation checks of customer’s telephone number, physical address and e-mail address.

- Screening for high risk international addresses.

Additional e-commerce/MOTO Merchant liability

By signing this Agreement, the Merchant declares to be using the Virtual terminal as indicated in the Merchant Application Form, where the Merchant is processing MOTO transactions, using the Payment Page as indicated in the Merchant Application Form, where applicable and Merchant shall be using payment gateway as indicated in the Merchant Application Form and is thereby fully compliant with the Payment Card Industry Data Security Standards (PCI DSS) and accepts all liability for losses resulting from compromised card data arising from failure to adhere to the PCI DSS.

The Merchant is required to record the voice conversation and/or keep a script of each MOTO transaction processed by the Merchant. PayAlly Limited reserves the right to request and listen into these recordings.

Where the merchant is using his own Virtual Terminal and/or his own Payment Page and in the event of an experienced or suspected security breach, the Merchant undertakes to immediately inform PayAlly Limited. The Merchant is to provide PayAlly Limited with a list of the

compromised accounts within 24 hours and an incident report within 4 business days of the reported compromise.

Where the merchant is using the provider's Virtual Terminal and/or the provider's Payment Page and in the event of an experienced or suspected security breach, the Merchant together with the provider jointly and severally undertake to immediately inform PayAlly Limited. The Merchant and provider are to provide PayAlly Limited with a list of the compromised accounts within 24 hours and an incident report within 4 business days of the reported compromise.

Where the merchant is using the third party's Virtual Terminal and/or a third party's Payment Page and in the event of an experienced or suspected security breach, the Merchant undertakes to immediately inform PayAlly Limited. The Merchant and provider are to provide PayAlly Limited with a list of the compromised accounts within 24 hours and an incident report within 4 business days of the reported compromise.

Other matters

Merchant Data Security Requirements - Payment Card Industry Data Security Standard (PCI DSS)

Merchants, provider and third party gateway performing card data processing, transmission or storage must ensure that they or, where they are using the hosting payment page of the provider, that said provider are in compliance with the 12 requirements of the PCI DSS 'control objectives' outlined in detail on the PCI council website: https://www.pcisecuritystandards.org/. PayAlly Limited may request a Merchant and/or Provider to provide validation of PCI compliance according to Industry requirements. Without prejudice to the obligation of compliance with the aforesaid, the following represent the key objectives to be complied with as set out in the said website:

- Build and Maintain a Secure Network

  Requirement 1: Install and maintain a firewall configuration to protect cardholder data

  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect Cardholder Data

  Requirement 3: Protect stored cardholder data

  Requirement 4: Encrypt transmission of cardholder data across open, public networks

- Maintain a Vulnerability Management Program

  Requirement 5: Use and regularly update anti-virus software

  Requirement 6: Develop and maintain secure systems and applications

- Implement Strong Access Control Measures

    Requirement 7: Restrict access to cardholder data by business need-to-know

    Requirement 8: Assign a unique ID to each person with computer access

    Requirement 9: Restrict physical access to cardholder data

- Regularly Monitor and Test Networks

    Requirement 10: Track and monitor all access to network resources and cardholder data

    Requirement 11: Regularly test security systems and processes

- Maintain an Information Security Policy

    Requirement 12: Maintain a policy that addresses information security.

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and if each data element must be protected.

	Data Element	Storage permitted	Protection required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name*	Yes	Yes
	Service Code*	Yes	Yes
	Expiration Date*	Yes	Yes
Sensitive Authentication Data**	Full Magnetic Stripe	No	N/A
	Card Verification data ***	No	N/A
	PIN/PIN Block	No	N/A

* *These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business.*

** *Sensitive authentication data must not be stored subsequent to authorisation (even if encrypted).*

*** *Card Verification data elements are as follows:*

CVV/ CVC = Card Verification Value in the magnetic stripe.
CVV2/CVC2 = Card Verification Value printed on the back of the card in or next to the signature panel.
iCVV = The Card Verification Value contained in the magnetic stripe image in a chip application.
PVV = PIN Verification Value contained in the magnetic stripe.

These security requirements apply to all “system components.” System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Pledge Agreement (Clients’ Account)

PayAlly Limited, shall hereinafter be referred to as the “Pledgee” The Merchant shall hereinafter be referred to the “Pledgor”
Jointly referred to as the “Parties”