BOI Payment Acceptance

Customer Operating Instructions

April 2017

A division of EVO PAYMENTS INTERNATIONAL

Contents

1. Welcome

Thank you for choosing BOI Payment Acceptance (BOIPA). We value your business and are fully committed to making card acceptance easy for you and your customers. In this guide you will find information that will help you, your staff and your business as you start your journey with us.

BOIPA is an alliance between Bank of Ireland and EVO Payments International, a leading player in the global payments industry. Together it is our goal to deliver innovative payments solutions and exceptional customer service to the Irish business community.

This guide will illustrate how your customers use our products and services when they are doing business with you.

1.1 Making the most of this guide

This guide will help you make the most of the benefits of accepting payments with BOIPA. Please read this guide carefully, as it will help you to:

- Accept card payments efficiently and smoothly
- Receive prompt payments to your bank account
- Protect your business by minimising the risk of losses caused by fraud and mistakes
- Understand your responsibilities

1.2 Our values

Ethical

At BOIPA, our commitment to operating ethically in everything we do is part of our core values. When you are dealing with the BOIPA team, whether they are part of our sales, customer service or engineering department, you can be sure that they are acting ethically and with the best interests of your business in mind.

Transparent

When you begin your journey with BOIPA, you join a team where everyone works together. We understand how you like to manage your business and run it efficiently and in a cost effective manner. Your account is always visible to you

in real time and you always know what you are paying for and why. In fact with BOIPA, the only surprise in store for you is our fresh approach in this Industry.

Innovative

Being innovative in our Industry means that you and your customers have a seamless card payment and settlement experience. Our commitment to technological innovation means that we are constantly building our portfolio of offerings so that you can take payments in an ever increasing number of ways whatever your business needs.

1.3 Point-of-sale display material

Before you begin to accept card payments you will need to take a few steps to ensure your customers are aware that they can use them at your shop or business. A well-designed point-of-sale (POS) display encourages increased spending. We can provide display materials that include shop-front window / door stickers and countertop material to show your customers that you accept card payments.

1.4 If you need to contact us

This guide should answer most of your questions about processing transactions. However, if you need any further help, please get in touch. We are open 24 hours a day.

Customer Support

1 800 806 670
Email support@BOIPA.com

Customer Sales

1 800 806 770

PCI

https://BOIPA.simplePCIDSS.eu

1.5 Other ways to contact us

We are also available on the web at www.BOIPA.com

To contact BOIPA in writing, please write to:

BOI Payment Acceptance,
The Observatory,
Sir John Rogerson's Quay,
D02 VC42, Dublin 2,
Ireland

2. Important Information

It is very important to read this information before you start taking card payments because it tells you more about your obligations. If you have any questions, please get in touch with us and we will be happy to help.

2.1 Your contract with us

This guide forms part of your Contract with us. It covers the services you have requested and may include some others. You must ensure that your card processing facility is only used to accept payments for the goods and/or services that

you told us your business provides. Taking card payments for goods and/or services without the knowledge and prior agreement from BOIPA may result in termination of your Contract with us.

2.2 You must tell us about any of these:

- If you change the nature of your business – for example, if you start selling a different kind of goods or services, begin trading online or offer guarantees or warranties
- If you change your website address and/or intend to sell via a new website address
- If you change the length of the guarantees or warranties offered on your products
- If you change the legal entity of your business – for example from sole trader to limited company
- Change to your bank account details
- Change of postal address
- Change of email address
- Change of contact name
- Change of contact number
- If a partner/director/owner changes name
- If a partner/director leaves or a new partner/director joins
- If you open or close an outlet/site
- If you do not want to take cards any more

You must provide notification to BOIPA of any changes to your circumstances, in writing and with an authorised signature. If you do not let us know about any of the above changes, we may suspend or withdraw some or all of your card-processing facility.

2.3 Your terminal is for business use only

You must not process any transactions that do not directly relate to the sale of goods and services provided by your business and for which you have a contract with us. You must never process transactions on behalf of third parties. This includes sales, purchase with cash back or refunds to your own card account or any other card. If you do not comply with your obligations, we may suspend or withdraw some or all of your card processing facility. We may also suspend or withhold some or all funds for the transactions processed through the facility. In addition you will also be liable for any card scheme fines in result of your actions. It is your responsibility to ensure that all of your employees comply with their obligations.

2.4 Minimising risk

You take card payments at your own risk. Risks can exist with all types of card payments but some are higher than others (for example, cardholder not present transactions). This document includes tips on how you might identify and reduce the risk of fraudulent transactions.

If you and your staff follow the instructions in this guide carefully, the risk may be reduced, but it' s important to understand that card payments are not guaranteed and that you carry the risk of chargebacks for fraudulent transactions. Even if a payment is authorised this simply means that at the time of the transaction, the card had not been reported as lost or stolen (perhaps because the genuine cardholder was not even aware of this at the time) and there were sufficient funds available to cover the transaction. Please make sure that everyone taking card payments for your business has read this guide thoroughly and practised the procedures. We also recommend you hold regular training sessions with all your staff to refresh their understanding. Much of the information and guidance provided in this Customer Operating Instructions Guide is based on what we believe is current industry best practice. We hope that such

practices will help you minimise possible exposure to security breaches or losses through fraud and chargebacks. Note: Authorisations do not guarantee settlement.

2.5 Card types

Remember you can only accept card types set out in your BOIPA contract. If you process any others, the transaction may be returned unpaid, either rejected during processing or returned via the chargeback process.

2.6 Keeping records

Terminal receipts, paper vouchers and other transaction records are high-security items and access to them should be restricted. Keep your copies of all transaction details in a secure place for at least 18 months in case there is a query later or the details are required to help to defend a chargeback.

Do not alter transaction records in any way. If there is a dispute, the cardholder' s copy will normally be taken as correct. After 18 months, make sure that you dispose of all transaction records securely.

2.7 Using your terminal

Depending on your terminal type, you may be required to provide a telephone line or internet service for your terminal to connect with the BOIPA Processing and Authorisation Systems. If your terminal is supplied by BOIPA you must ensure that it is connected and powered on at all times to ensure it is available to receive important updates if required. Mobile terminals operate over GPRS (mobile data network). Whilst normal mobile phone connectivity is a good indicator of service, GPRS coverage and connectivity cannot be guaranteed.

2.8 Authorisation of transactions

Authorisation of a transaction confirms that at the time the transaction was taken the card has not been reported as lost or stolen and there are sufficient funds available to cover the transaction. It does not confirm the authenticity of the card presenter or the card, nor does it guarantee payment.

2.9 How to receive your funds

Receiving your money is probably the most important part of the overall process for you. This is what we refer to as settlement.

In order to receive your daily funds, a batching process needs to take place that will initiate actual money flow. This is usually performed at the end of your business day and therefore often referred to as end of day batching. All our terminals perform an automatic batch run at midnight to make sure that you receive your funds as soon as possible. If desired, you can also start a manual batch from the terminal menu whenever it suits you. For e-commerce scenarios the batching process depends on the individual setup.

Once the batch has been performed, the financial institutions start processing the transactions, then settle the transactions of all the customers with us so that we can start paying out the funds to the nominated customer accounts.

If you nominated a Bank of Ireland account you will receive the funds within one working day after the batching of the transaction, if the batching day is a working day also. If transactions are processed and batched over the weekend for example they would go into processing over the weekend and settled on Monday.

For accounts of other banks funding will happen within 3 working days after the batching of the transaction.

3. Payment And Information Security

The Card Schemes have set out mandatory information security requirements to help make sure that sensitive cardholder information remains safe including while storing, processing and transacting cardholder data. The requirements are regulated by the PCI Security Standards Council (PCI SSC). All customers must comply with these requirements and certify compliance annually. We will be in contact with you shortly after initial installation and annually thereafter to assist with the self-certification process. As a card acquirer, BOIPA has a responsibility to report our customers' PCI DSS compliance status to the Card Schemes (including Visa & MasterCard).

In addition to confirming your compliance annually, it is equally important to ensure that this degree of protection is maintained long term. PCI DSS is intended to protect your business and customers against real data security risks.

4. Card Present Transactions

These are face-to-face transactions where your customer and their card are with you at the point of sale.

4.1 Chip and PIN and Contactless

Chip and PIN and Contactless are the usual ways to accept card payments on your terminal when the card and cardholder are present. Some cardholders, however, will continue to sign to authorise payments and this could be due to an impairment that prevents them from inputting their PIN or because their card does not support Chip & PIN technology. Some cardholders will still have magnetic stripe only cards and these must not be refused at the point of sale.

Before you start

> Are you sure that the card belongs to the person presenting it? If you are unsure, call BOIPA Customer Support and say that "This is a 'Code 10' call".

4.1.1 A step-by-step guide (Chip and PIN)

- Following the terminal prompts, key in the full amount of the transaction
- Ask the cardholder to either insert their card into the chip reader slot on your terminal or PIN entry device
- Your terminal will now usually ask the cardholder to enter their PIN. If it doesn't, this could be because the cardholder has a card that does not support chip and PIN technology (such as a chip-and-signature or magnetic-stripe-and-signature card). Your terminal will advise which method is required – always follow the prompts on the terminal
- Ask the cardholder to check that the transaction amount is correct and to enter their PIN
- Most terminals will then authorise the transaction automatically. If the terminal prompts you, call our Authorisation Centre immediately and follow the instructions
- Wait for the terminal to print out a terminal receipt
- Only give the cardholder the goods they are buying when you have received authorisation and completed the transaction. If authorisation is not given, do not go ahead with the transaction. Ask your customer for an alternative payment method
- Ask the cardholder to take their card from the terminal and give them their copy of the terminal receipt

Keep your copy of all terminal receipts in a secure fireproof place for at least 18 months in case there is a query later or these details are required to help defend a chargeback. Do not alter them in any way. If there is a dispute, the cardholder's copy will normally be taken as correct.

Remember that even where authorisation is given, this is no guarantee of payment and the transaction is still open to being charged back.

4.1.2 A step-by-step guide (Contactless)

Contactless is an increasingly popular method of payment and all BOIPA POS terminals have contactless functionality. Contactless cards enable purchases under €30 to be completed by tapping the card over a Contactless reader on the enabled terminal. This improves the customer payment experience, speeds up transactions and helps retailers to remove cash from their business.

- Key the full amount of the transaction into the terminal
- If cardholder has a Contactless card (check for Contactless symbol – see above), the cardholder will be able to tap the card against the Contactless reader
- Most terminals will authorise the transaction automatically
- Wait for the terminal to print out a receipt
- Only provide the cardholder with the goods, or services they are purchasing when you have received authorisation and completed the transaction

All BOIPA terminals support Apple Pay and Android Pay transactions. To pay, the customer just holds their Phone near the contactless terminal reader for transactions under €30. For transactions over €30, the customer must unlock their phone using their PIN or touch ID. The terminal will make an audible beep when the transaction is approved in the same manner as for a normal contactless transaction using a card.

4.2 When a signature is needed

You should only use a signature to verify a transaction when prompted by your terminal. In addition, when processing a refund, you (rather than the cardholder) will be required to sign the receipt and the transaction will not require the input of the PIN.

4.2.1 A step-by-step guide (when a signature is needed)

- Following the terminal prompt, key in the full amount of the transaction
- Insert the card and follow the terminal prompts which will tell you when a signature is required
- Most terminals will then authorise the transaction automatically. If the terminal prompts you to, call BOIPA Customer Support immediately and follow the instructions
- Wait for the terminal to print out a terminal receipt

- Check that the card number, expiry date and card type on the terminal receipt are the same as on the card. If any details are different, hold onto the card and cancel the transaction immediately. Then call BOIPA Customer Support and say that "This is a 'Code 10' call" (see below).
- If all the details match, check the transaction and amount, then ask the customer to sign the terminal receipt.
- Check that the signature matches that on the card. If you are not sure, you may decide to ask for additional identification such as a driving licence or a passport. If you are still in doubt call BOIPA Customer Support
- If you are happy with the signature, confirm the transaction on the terminal and give your customer their card and receipt
- Only give the cardholder the goods they are buying when you have received authorisation and completed the card transaction. If authorisation is not given do not go ahead with the transaction. Ask your customer for an alternative payment method

Code 10 Calls

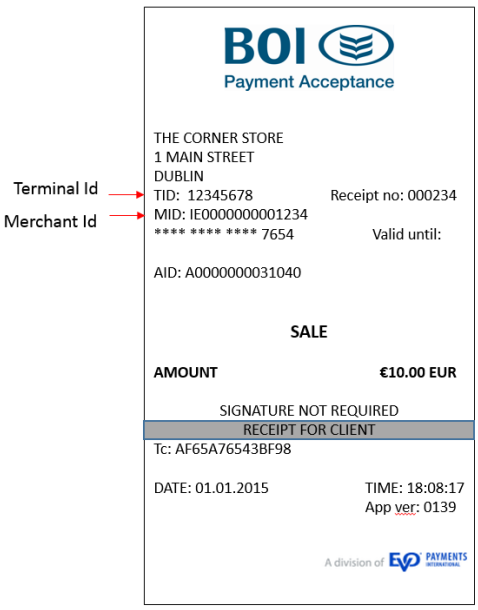
If you're in any way suspicious about a card, the cardholder or the circumstances surrounding a transaction, you can call the Customer Support Team. A 'code 10' allows you to discreetly check on a suspicious card or cardholder when they're nearby and you're not able to talk freely. Just call our Customer Support Team and tell the operator you're making a 'code 1' 0 call. You'll be asked for the card number, the expiry date and the issue number (if applicable) and given options to choose from, depending on the type of call you are making. You will be asked a series of questions that require only a yes or no answer. Remember to keep the card and the goods out of reach of the customer and activate any surveillance equipment you may have. If the operator asks you to keep the card, inform the customer politely, without putting others or yourself at risk. Please note that 'Code 10' is only available for customer-present transactions, not for mail, telephone or internet transactions.

4.2.2 Extra security checks

If you do carry out a transaction using a signature as verification, you should take extra security precautions. Here are some basic ones:

- Make sure the card is not damaged, cut or defaced in any way
- Check the signature strip for signs of damage or tampering
- Check any specific security features for that card
- Ask for some photo Id if you are in doubt
- If you are unsure make a 'Code 10' call

4.3 The Receipt



4.4 Troubleshooting

You must always follow the prompts on your terminal and never try to avoid using the higher-level security features (such as chip and PIN).

If the cardholder enters their PIN incorrectly

The cardholder will usually have three chances to enter their PIN. If all these fail follow the prompts on the terminal which will show whether the transaction can be completed on the card or if the cardholder will need to provide another means of payment.

If the cardholder has forgotten their PIN

If your terminal allows PIN bypass follow the terminal instructions. If your terminal does not allow PIN by-pass ask the cardholder for another means of payment.

If you receive a message that the PIN is locked

Please advise the cardholder to get in touch with their card issuer and ask for a new PIN, so that they can start using the card again in the future.

If the chip reader does not work

If the card offered contains a chip, the card must be entered into the chip card reader. If a terminal message says the card cannot be read:

- Insert the card again (or try again with the card the other way round)
- If this doesn' t work the card may be damaged and you can try to swipe the card instead
- If the card is still unable to be read ask the cardholder for an alternative payment method

Please note: if you swipe or key enter a chip card and the transaction is later found to be fraudulent, the transaction may be charged back to you.

4.5 Terminal Options

You can choose between the following terminal models.

			
	Counter Top	Portable	Mobile
Terminal Type	iCT220+Pin Pad	iWL220 with base	iWL220
Industry Examples	Retail Outlets	Hospitality	Taxis Tradesmen Mobile Services
Card Readers	Contactless Chip Reader Magstripe Reader Manual Key Entry	Contactless Chip Reader Magstripe Reader Manual Key Entry	Contactless Chip Reader Magstripe Reader Manual Key Entry
Printer Speed	18 lines/sec	18 lines/sec	18 lines/sec
Printer Roll Spec	Thermal 57x40x12mm	Thermal 57x40x12mm	Thermal 57x40x12mm
Available Colours	Black	Black	Black
Display Type	Monochrome Graphic	Monochrome Graphic	Monochrome Graphic
Customisable Receipts	Yes	Yes	Yes
Connectivity Options	GPRS Dial-Up Ethernet	Bluetooth Wi-Fi	GPRS
Battery Life	Connected to Mains	6 Hours 200 Transactions per charge	6 Hours 200 Transactions per charge
Language	English	English	English
Keypad	15 Operational Keys 4 Navigation Keys	15 Operational Keys 7 Navigation Keys	15 Operational Keys 7 Navigation Keys

5. Authorisation and Referrals

Authorisation and referrals are ways of checking that at the time of taking the transaction the card has not been reported lost or stolen and that there is enough money in the account to cover the purchase. It' s important to understand that authorisation does not guarantee payment.

5.1 Making a referral call

In the majority of cases the authorisation check is automatic. Sometimes your terminal will prompt you to make a manual authorisation call, known as a referral. If you have a mobile or portable terminal, this will have been handed to the customer to input their PIN. You must always take back the terminal from your customer as soon as the PIN is entered. That way you will know whether the transaction has been authorised or whether a referral call needs to be made. You must make this call at the time of transaction, while the cardholder is present, and you are holding the card. Do not hand the card back to the customer until you have received authorisation and the code has been accurately keyed into your terminal.

Security questions

During some calls, the cardholder may need to answer one or more personal security questions. Explain that this is part of the card issuer' s i.e. the Bank that issued the credit/debit card to the customer, standard security procedures. BOIPA Customer Support will usually ask to speak to the cardholder directly. Once your customer has answered the questions, they should pass the phone back to you. You should not use any information which is given to you by the cardholder. Only BOIPA Customer Support can give you an authorisation code. You must not accept an authorisation code from anyone else (especially your customer).

If the transaction is authorised

You will be given an authorisation code which should be keyed into your terminal when you are prompted. There's more information in your Terminal User Guide about keying the code.

If the transaction is declined

- Explain that the transaction has not been authorised and give the card back to the customer, unless BOIPA Customer Support asks you to retain it and it is safe to do so
- If your customer asks why, advise them to contact their card issuer – there is normally a helpline number on the back of the card
- Remember, transactions are declined for many reasons – it may not be your customer' s fault
- Make sure you destroy any partially completed sales vouchers in front of your customer
- If your customer still wants to go ahead with the purchase, ask them for an alternative payment method. Remember to check any new card carefully

5.2 Suspicious transactions

If you are suspicious about a transaction, follow the procedures to make a 'Code 10' call.

5.3 Transaction changes after authorisation and before processing

Sometimes, you need to make changes to a transaction after you have obtained authorisation. For example, if your customer decides to buy something different, or not to go ahead at all. If you process payments electronically, you can cancel the sale on your terminal and it will make the adjustments automatically, but this may take a few days to appear on the cardholder' s statement.

5.4 Split transactions

You must not split the sale into two (or more) separate amounts on one card in order to avoid obtaining authorisation for the full amount. If a sale is split in this way you may be at increased risk or receiving a chargeback for which you will be liable.

6. Refunds

When you make a refund on a card transaction, the amount of the refund is returned to the customer' s card account and a corresponding debit will be made to your nominated bank account. If the refund facility is used where there is no corresponding originating transaction, this is not a Refund within the meaning of your contract and this is a breach of your contract for which you will be responsible.

6.1 Before making a refund

Never make a refund unless there was an original purchase. If you do, we may withdraw your card processing facility. We may also suspend or withhold some or all funds for the transactions processed through the facility

- Check that your customer has given you the card used for the original transaction – we recommend that the refund is made back to the card used for the original purchase where it is still available. If however such card is not available at the time of refund then you may, at your discretion, use alternate means to issue such refund
- Never give a cash or cheque refund for a card transaction – fraudsters often try to obtain cash this way
- If the customer has received a replacement card, the card number may have changed. In this case, take reasonable steps to make sure you refund to the original account. For example, check that the start date of the new card is after the purchase date, and ask them for proof of identity
- If the card has expired, you should still make the refund back to it, letting your customer know that they need to contact their card issuer to arrange for the funds to be received

Please note: you could be at risk of a chargeback if a refund is not made to the original card used for the purchase.

7. Card Not Present Transactions (CNP)

Card not present (CNP) transactions are those where the card and cardholder are not with you at the point of sale. Offering your customers this option gives extra flexibility, but it' s important to understand that you will need BOIPA' s agreement to accept these transactions:

- Mail Order Telephone Order Transactions
- eCommerce Transactions

7.1 Can I accept CNP transactions?

Before deciding to accept CNP transactions you should consider all risks to your business, because they carry a higher risk of fraud and you will be financially liable if a transaction is confirmed as invalid or fraudulent. You can only accept CNP transactions if you have signed up to this with BOIPA. If you have not, but you would like to make CNP sales, please contact the BOIPA Customer Support Team.

7.2 Authorisation

As with other transaction types, all CNP transactions must be authorised. Authorisation is not a guarantee of payment – Authorisation simply means that at the time the transaction was taken and you obtained authorisation the card has not been reported lost or stolen and there are sufficient funds available. Authorisation cannot always validate the address you have been given and therefore you should consider undertaking additional checks as appropriate.

8. Additional services

The following services are not activated on our terminals as standard and subject to approval. If you want to use them, please contact our customer support team.

8.1 Cashback

Cashback allows you to offer up to €100 in cash on top of any debit transaction. This way you are not only offering your customers a highly attractive service, you are also retaining less cash in-store and reducing costs associated with cash handling with your bank. And the best of it all is that it is free of charge for you.

Note: Cashback is not a feature of credit cards and is only available on domestic issued cards, from Republic of Ireland.

8.2 Dynamic Currency Conversion

Dynamic Currency Conversion (DCC) enables your International cardholders to pay in their home currency while you will receive funding of the original sale amount in Euros. If for example a British customer presents a card that is issued in Sterling, the terminal will recognise it and will offer the cardholder to pay in Sterling. If this option is selected, an immediate currency conversion into Sterling is performed, showing the exact amount in Sterling like it will show up on the customer's card statement.

Advantages for your customer:

- Actual understanding of prices in foreign countries
- Easier management of business expenses for your business customers
- Easier to recognise foreign transactions on the card account statement

Advantages for your business:

- Better customer experience as they have a full understanding of the item cost in their home currency
- Fewer chargebacks as transactions are more likely to be recognised on the card account statement
- A percentage of the DCC transaction is paid to the merchant

DCC is available in the following currencies:

Country	Currency
UAE	U.A.E. Dirham (AED)
Australia	Australian Dollar (AUD)
Bulgaria	Bulgarian Lev (BGN)
Brazil	Brazilian Real (BRL)
Belarus	Belarussian Ruble (BYR)
Canada	Canadian Dollar (CAD)
Switzerland	Swiss Franc (CHF)
China	Chinese Yuan (CNY)
Czech Republic	Czech Koruna (CZK)
Denmark	Danish Krone (DKK)
EU	Euro (EUR)
Britain	British Pound Sterling (GBP)
Croatia	Croatian Kuna (HRK)
Hungary	Hungarian Forint (HUF)
Iceland	Iceland Krona (ISK)
Israel	Israeli Sheqel (ILS)
Japan	Japanese Yen (JPY)
South Korea	South Korean Won (KRW)

Country	Currency
Kazakhstan	Kazakhstani Tenge (KZT)
Lithuania	Lithuanian Litas (LTL)
Mexico	Mexican Peso (MXN)
Norway	Norwegian Krone (NOK)
Qatar	Qatari Riyal (QAR)
Romania	Romanian Leu (RON)
Russia	Russian Ruble (RUB)
Saudi Arabia	Saudi Riyal (SAR)
Sweden	Swedish Krona (SEK)
Turkey	New Turkish Lira (TRY)
Ukraine	Ukrainian Hryvnia (UAH)
United States	U.S. Dollar (USD)
South Africa	South African Rand (ZAR)

8.3 Tips/Gratuity

If accepting tips is important for your business we can set up a facility on your terminal to accept tips and gratuities free of charge.

8.4 MOTO (Mail Order / Telephone Order)

If your business receives orders by Internet, mail or telephone, you can still process card transactions by enabling the MOTO service. This allows you to process transactions without the cardholder and their card being present in your place of business.

The key difference between regular transactions and MOTO transactions is that the cardholder and their card are not normally present. To process a MOTO transaction, you will need to take the cardholder' s:

- Card number - the long number across the centre of the card
- Name as it appears on the card - including any initials
- Card expiry date
- Full postal/billing address, including postcode, as it appears on the cardholder's statement
- Chosen delivery address - if different from above
- Card Security Code (CSC) - three-digit code at the end of the signature strip (NOTE: CSC needed for telephone order transactions only, NOT required for Mail Order transactions)

9. Pricing

At BOIPA we offer two distinct pricing options - Ready Made and Tailor Made. Ready Made is suitable for merchants with monthly card payments of €8000 or less. Tailor Made pricing is suitable for all other merchants. Refer to your contract for further details of your particular pricing package.

9.1 Changing your package

Changing up and down between Ready Made packages to suit your business requirements is easy. The change of plans will take about 5 working days but will only come into force for the next monthly billing period. If you want to switch for the next month, please make sure that you give us notice early enough prior to end of month. Otherwise the switch to the new plan will be performed a month later.

9.2 Terminating your BOIPA account

You may terminate the agreement at any time for any reason subject to one month' s notice to us. To do so, please contact our customer support team.

If your contract term has not expired on date of account closure you are liable for terminal rental fees for the remainder of your contract terms. For all Ready Made plans a termination fee of €150 will be charged on early account closure.

10. eCommerce Transactions

We provide a range of services to enable you to trade online. Our gateway solutions are designed to simply connect to your eCommerce store.

10.1 Important

- Before you can make eCommerce sales, you need an agreement with BOIPA that allows you to accept Ecommerce transactions.
- When this arrangement is in place we will give you guidance about setting up and integrating your website with our gateway.
- You must always advise BOIPA if you intend to take transactions from a new website we had no prior knowledge of.

10.1 Payment types you can accept

Our Gateway solutions allow you to accept a wide range of credit and debit cards, including:

- Visa Debit and Credit
- MasterCard Debit and Credit
- Maestro
- Visa Electron

10.2 Reducing fraud and chargebacks

Most eCommerce sales are genuine. However, because the Internet is relatively anonymous – you don' t see the card or the shopper – some people see it as a less risky way to attempt fraud. Fraudsters want to obtain goods they can sell on for cash; others 'card test', placing an order to check if the card details they have will be authorised. If an eCommerce transaction is disputed, it is very difficult to prove that the real cardholder ordered the goods and you will be responsible for any challenge raised. To reduce the risk of fraud and chargebacks, it is extremely important to follow the correct procedures.

When making an eCommerce sale, you must do all you can to check your customer' s identity and make sure that they are entitled to use the card being offered. If you employ a third-party Payment Service Provider (PSP) to capture and process your eCommerce transactions, they should deal with the below process for you. Note that you should only use a PSP that is compliant with the PCI DSS requirements. Details to collect:

- Card number
- Card expiry date
- Cardholder' s name and initials as they appear on the card
- Cardholder' s full postal address/billing address
- Delivery address, if different
- Card Security Code (if your PSP software is enabled to capture these details) – the last three numbers on the signature strip (Please note: This information must only be used for one transaction and must not be stored for future use)

10.3 Cancellations after an eCommerce order is taken

- If an eCommerce transaction is cancelled for any reason and the original transaction was authorised, you must let BOIPA Customer Support know or refer to your implementation pack for contact details
- If you employ a third-party Payment Service Provider to capture and process your eCommerce transactions, you must also let them know that the transaction is cancelled
- If the transaction has already been processed, you will need to make a refund

10.4 Keeping customer data secure

- Card details must be captured and stored securely, either on your own secure server or by a PSP able to connect to BOIPA
- Card details must always be encrypted and the host server must be protected by a firewall
- E-mail is not a secure way to transfer card transaction data. You must ensure that the card number is omitted from the order confirmation message sent to your customer

11. Reducing Fraud

Card Present Transactions

These are face-to-face transactions where your customer and their card are with you at the point of sale.

Card Not Present Transactions: Mail Order Telephone Order

These are sales made by mail or over the telephone where the customer and their card are not with you at the point of sale.

Card Not Present Transactions: eCommerce

These are sales over the Internet where the customer and their card are not with you at the point of sale.

Card fraud is becoming increasingly sophisticated and, if you are not vigilant, can result in financial loss for your business. Your exposure to fraud will depend upon how aware you are of the risks and how carefully you and your staff handle card transactions. This section gives you some useful tips to help you reduce your risk of losing money through fraud. Before deciding to accept CNP transactions you should consider all risks to your business, because they carry a higher risk of fraud and you will be financially liable if a transaction is confirmed as invalid or fraudulent.

11.1 Always remember

- Follow all the prompts on your terminal
- Be alert and aware – for card present transactions, if you are suspicious about a card or the person presenting it, make a 'Code 10' call and follow the prompts
- Be discreet when you are suspicious – don' t take risks with anyone' s safety

- If your terminal has a supervisor card or code, keep it safe and secure – anyone who has access to this could make fraudulent refunds to a card which may result in financial loss for your business
- Never allow a third party to authorise or process card transactions using your facility – this would breach your contract with us and may result in withdrawal of your facility and/or in Card Scheme fines. You will be liable for any fraud/chargebacks irrespective of the fact you have processed transactions on behalf of someone else
- Keep your terminal in sight during a transaction and take it back from your customer as soon as they have entered their PIN

11.2 Training your staff

Alert, well-trained staff members are your frontline defence against card fraud and can significantly reduce the risk of financial loss to your business. If you or your staff allows fraud to take place through carelessness, you could lose money and we may even stop processing card payments for you. Please make sure your staff read this guide carefully, and any other fraud prevention publications we send you.

11.3 Withholding payments

If we are suspicious about a transaction you have processed or we believe that a transaction may be fraudulent, we may hold back payment while we investigate. The money will not be returned until we have confirmed that a genuine transaction has been processed and it was for the goods or services provided by you (and not any third party) and which you advised you would be providing on your application form. There is no set time limit for the investigations to be resolved, but we will keep you informed throughout.

11.4 Card present transactions

These are face-to-face transactions where your customer and their card are with you at the point of sale.

11.4.1 Look out for fraud warning signs

Be aware of how customers normally behave when they are shopping. If you notice anything out of the ordinary, or something that just doesn't feel right, it could be a sign of potential fraud, so act on your instincts and don't go ahead if you are suspicious. Look out for…

- Random, careless or bulk purchases – Most customers ask questions and, for example, try on clothing, but a fraudster will just buy goods that can be easily re-sold
- Rapid repeat visits – A customer who returns to buy more in a short period of time may be making the most of the fact that the card has been accepted already
- Nervous or hurried customers – They may be worried about being caught
- Cards signed in felt-tip pen – This can be used to disguise the original signature – remember all cards should be signed in ballpoint pen
- Interruptions – A customer who tries to distract you during the transaction, and who seems fully conversant with how the authorisation process works, may be trying to prevent you from noticing something suspicious. Never turn your attention away from the terminal once you have started processing the transaction, as you may miss prompts on the screen, or miss a fraudster attempting to interfere with the terminal
- Fake authorisation calls - Neither BOIPA nor the card issuing bank will EVER call you during the processing of a transaction to provide you with an authorisation code. If this happens this will be an attempt by fraudsters to force through a transaction, and will result in a loss to your business if the transaction is charged back. If you receive one of these calls please cancel the transaction (if safe to do so) and perform a 'Code 10' call
- BOIPA, Police or other 'official' impersonation – You should never receive a phone call from the BOIPA authorisation centre, the police, your terminal provider or any other official, requesting you to provide any card

details over the phone. None of these organisations will ever ask for details over the phone, so these will be an attempt by fraudsters to gain card details from you. If you receive one of these calls, please report it to the BOIPA Helpdesk

11.4.2 Take extra care when a signature is needed

Nearly all cards now use chip and PIN technology, but you may sometimes come across cards that need to be verified using a signature rather than a PIN. Knowing when these cards can be used and their security features will help you to identify genuine transactions and also to spot potential fraud. Take extra care when accepting these transactions because you could be financially liable if a transaction is confirmed as invalid or fraudulent. In certain circumstances, you can accept:

> Magnetic stripe and signature cards – These will mostly be non-ROI/UK issued cards from countries that have not yet upgraded to chip and PIN. Follow the prompts on your terminal

11.4.3 Some basic fraud checks to use when a signature is required

If you do carry out a transaction using a signature as verification, you should take extra security precautions:

- Check the security features of the card
- Check the cardholder's signature matches that on the back of the card
- If possible, check that the spelling on the card is the same as the signature – fraudsters sometimes don't spell the name correctly
- Check the title on the card matches the gender of the person presenting it
- Check the signature strip for tampering – has another strip been placed over the top of the original one? If the word "void" appears on the strip, this could be an indication that the genuine signature has been removed and a substitute used
- If you have an ultraviolet (UV) lamp, put the card under it and check the appropriate inbuilt security feature
- While the point-of-sale receipt is printing, check the last four digits of the card number on the receipt match those on the front of the card. If they don't, make a 'Code 10' call

11.4.4 If BOIPA Customer Support asks you to retain the card

Explain politely that the card issuer has asked you to hold onto the card. Your own company policy will decide whether you detain the cardholder or call the police. Never put yourself, your staff or the public at risk. Even if BOIPA Customer Support does not ask you to retain the card, you may decide that a card or a transaction is suspicious – for example, if you have identified it as counterfeit. Card thieves act fast, and will often try to use a card before the owner notices that it has gone.

11.4.5 Preserving evidence

The physical card which is presented to you and used fraudulently may need to be used as evidence. Treat them with care and you will make it easier for the police to catch and prosecute the thieves.

11.4.6 If someone leaves a card behind

- Keep it somewhere safe for at least 24 hours, in case the cardholder comes back for it
- If someone comes to claim the card, ask them for signed proof of identity, such as a driving license or other cards, and compare the signatures
- Ask them to sign a blank receipt and compare the signatures. Then destroy the receipt
- If you are then happy with the cardholder's identity, give them the card
- If you are suspicious, ask them to come back with additional proof of identity. If you are still not satisfied when they come back, call BOIPA Customer Support and say "This is a 'Code 10' call". The operator will talk you through the process
- If the cardholder does not return to reclaim the card, please send it to us to be cancelled. First cut the card into two pieces. Looking at it from the front, cut off the bottom left-hand corner. Do not cut through the signature

strip, magnetic stripe, hologram or chip. Then send the pieces with a short note giving your address and the date you found the card to:

11.5 Card Not Present Transactions (CNP)

If you are suspicious of the card, cardholder or circumstances of the sale at any time we recommend you do not continue with the transaction or send out the goods. If you decide not to proceed once you have already processed the transaction, you will need to make a refund to the card. CNP transactions are considered high-risk because you have no opportunity to physically check the card or meet the cardholder. Although most CNP sales are genuine, this type of transaction is appealing to fraudsters who want to obtain goods to resell easily for cash. So take extra care and consider the risks before you process CNP payments, because you will be financially liable if a transaction is confirmed as invalid or fraudulent.

11.5.1 Look out for fraud warning signs (MOTO)

Here are some signs that a transaction is likely to be fraudulent. Get to know them and make sure that all members of your staff recognise them too. Sometimes the first sign of fraud can just be a general feeling that something isn't quite right. If that happens, act on your instincts and don't send out the goods until you've carried out further checks.

- Multiple or bulk orders – Watch out for customers buying lots of the same item – either in the same transaction or separately
- First-time customers who place multiple orders – The risk of fraud is smaller when dealing with customers you know
- High-value orders – Orders larger than normal may indicate fraud. High-value items such as jewellery or electrical goods are often targeted by fraudsters because they are easy to resell, so take extra care with this type of transaction
- Hesitant customers – Customers who seem uncertain about personal information, such as their postcode or spelling of their street name, could well be using a false identity. Also watch out for customers being prompted when giving the requested information
- Same name, different title – Could your customer be using the card of a family member?
- Sales that are too easy – Be suspicious if a customer is not interested in the price and/or detailed description of the goods, but is only interested in delivery times
- Suspicious card combinations such as:
  - Transactions on several cards where the billing address matches but different/various shipping addresses
  - Multiple transactions on a single card over a very short period of time
  - Multiple cards beginning with the same first six digits offered immediately after the previous cards are declined
  - Customer offering multiple different cards one after another without hesitation when previous cards are declined
  - Orders shipped to a single address but purchased with various cards
  - Overseas shipping address – Be careful when shipping overseas, especially if you are dealing with a new customer or a very large order
  - Different shipping address – Orders where the shipping address is different from the billing address may be legitimate (for example, when sending flowers or a birthday present) but requests to send goods to hotels, guest houses or PO boxes are often associated with fraud

11.5.2 Look out for fraud warning signs (eCommerce)

Here are some signs that an eCommerce transaction is likely to be fraudulent. Get to know them and make sure that all members of your staff recognise them too. And remember that the first sign that something is wrong can just be a general feeling of unease. If that happens, act on your instincts and carry out further checks.

- A risk alert from the payment service provider or acquiring bank. This indicates that there is a cause for concern and that further checks are required before an order is fulfilled

- Multiple transaction attempts using the same or similar shopper details, such as name, e-mail address or IP address across one payment
- Different shopper details with one element the same – such as ten transactions from the same IP address giving different shopper names and e-mail addresses
- Multiple cards used by same shopper, especially where the card numbers are similar
- Obvious 'card testing', where the last four or eight digits of cards in a series of attempted payments contain similar numbers, or the card numbers are cycled repeatedly in a rough pattern or sequence
- Nonsensical shopper details, such as 'dgsgsgdf@dsgsd.com' as a shopper e-mail address or 'gdfgdfgfg' as a shopper name or billing address
- High-value transactions, especially where the amount is out of the ordinary for your usual daily processing amounts
- Mismatching Card Security Code (CSC) or mismatching Address Verification Check (AVS). Consider rejecting orders that carry mismatches or carry out further checks
- Mismatching combination of billing country, issuer country and IP country, especially, but not limited to, instances where the payment details are from any country or area which is associated with high risks of online fraud
- A delivery country that's out of the ordinary for your business and regarded as high-risk

12. Chargebacks

Card transactions are sometimes disputed by the cardholder or the card issuing bank, for example goods not received, transaction not recognised or authorised. When this happens we may contact you requesting further information. If you are not able to supply the information requested by us or in the timescales we specify then it is likely that this may turn into a chargeback which you may be held liable for, even if you have proof that the transaction was genuine.

Where there is a valid chargeback we will write to you to let you know and BOIPA will debit your nominated bank account with the value of the disputed transaction, quoting the same unique reference number as in the chargeback letter. You are responsible for making sure sufficient funds are in your nominated bank account to meet the chargeback. Failure to do so could result in your card processing facility being withdrawn.

12.1 Why chargebacks happen

Here are some of the most common reasons for chargebacks, but this is not a full list. If you are not sure about the reason for a chargeback, please contact BOIPA Customer Support.

12.2 Disputed payments

Some common reasons for disputes include:

- The cardholder claims someone was using the card without his/her knowledge or states that he/she does not recognise the transaction. It could have been stolen and used fraudulently – particularly for MOTO and eCommerce transactions
- There is a processing error, such as the wrong card number or wrong amount was keyed
- The cardholder disputes some other aspect of the transaction, for example non-delivery, late delivery, unsatisfactory goods or services, or the wrong size/colour/price

12.3 Wrong or suspect card details

There is also a high risk of a chargeback if there was a mistake when the transaction took place. Other common problems are:

- The card is not valid – for example it is out of date
- No signature
- Details on the terminal receipt or voucher don't match the card – i.e. the embossed details on the card do not match the details on the electronic receipt or the details have been entered incorrectly by hand -Primary Account Number (PAN) key entry
- Wrong process

- Your customer has been billed twice for the same sale
- The transaction was by PAN key entry, but a separate imprint and signature was not taken on a back-up paper voucher
- The sale required authorisation but it was not obtained
- An authorisation call was made, but the sale was not authorised

12.4 Goods and services disputes

These types of chargeback disputes can be difficult to defend and therefore if a customer contacts you with a dispute you should retain accurate records of what is discussed or agreed. Where possible, ask the customer to put the complaint or query in writing/e-mail and have the customer agree in writing to any resolution agreed. Proving the content of a telephone conversation at a later date is virtually impossible and the Card Schemes do not accept recordings of telephone conversations as evidence. It is important to be aware that the cardholder does not always have to physically return the goods to you for a chargeback to be correctly raised. Please also be aware that the use of 3D Secure protects you from fraud-related chargebacks, however chargebacks could still result from goods and service disputes.

12.5 Disputing a chargeback

You can dispute a chargeback that has been applied to your bank account. You will need to provide information to prove that the transaction was authentic. BOIPA will consider any information you can provide within the required timeframes proving that the transaction is authentic. However your account will only be credited if the evidence provided meets the rules set by the Card Schemes. Even if all procedures have been correctly followed and documented, this does not guarantee that you will succeed in disputing a chargeback. The technology we use is designed to ensure that chargeback enquires are resolved efficiently with minimum disruption to your business.

13. Card Recognition Guide

The majority of cards you see will be processed as chip and PIN or contactless and will not require you to have sight of the card. However, if the transaction is not completed by entering PIN or the card is a signature-only card, you will need to verify that the signature on the receipt matches that on the card. As more and more cards are introduced into the marketplace, you will be presented with cards of various shapes, sizes and colours. Provided you ensure that all the security features are present, including those specific to the individual card schemes, you can accept the card for payment. We recommend that all your staff know the process for accepting card payments, be familiar with these security features and always follow the prompts on your terminal.

13.1 Not a chip and PIN card or Contactless card?

Most cards are now chip and PIN and/or Contactless enabled, but you may sometimes be presented with chip and signature or magnetic swipe and signature cards. You must accept these cards as long as you verify the card and ensure that it has all the security features explained in this section, including those specific to the individual card schemes.

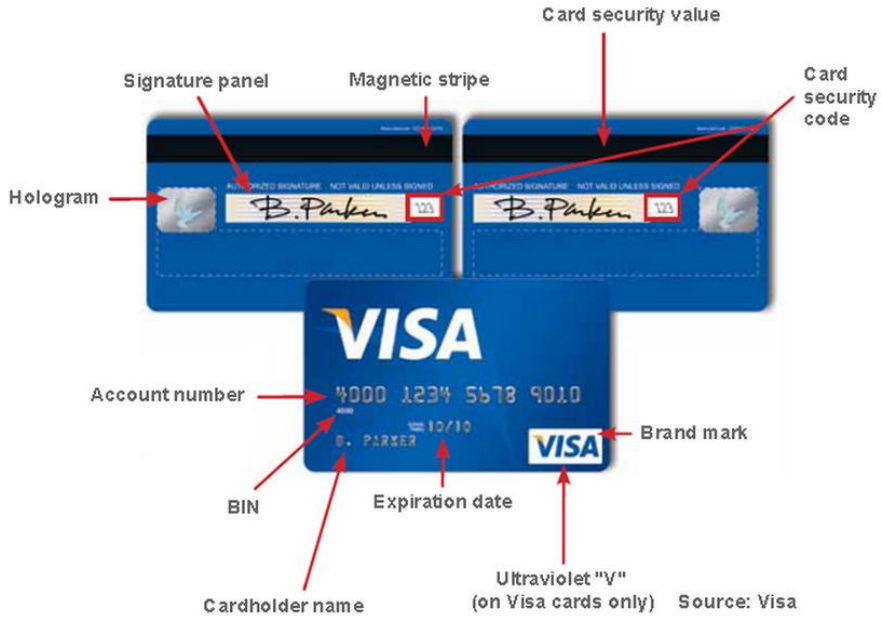
13.2 Key security features

As cards are normally placed in or tapped against card readers by the cardholder, you may not have the opportunity to check all of these security features, but these are the key details to check if you have any suspicions. Note that not all cards are embossed or have a full account number or cardholder name, but genuine cards will always have a:

- Card logo – see examples below
- Hologram – see examples below
- Ultraviolet image
- Card Security Code (CSC) - A three-digit code at the end of the signature strip or in a separate white box next to it.

13.3 Example cards

To see images and details of example cards please connect directly to the applicable Card Scheme web sites or view the sample Visa card below



13.4 What to look out for?

- Chip - If there is a chip; check if there is any visible damage
- Card number - The card number - the long number on the front – should be clear, even and in line
- The first four digits of the card number - Will be laser-imprinted on the front of the card beside the embossed details and should be identical to the embossed details (smaller type, above or below the beginning of the long embossed number)
- Cardholder title and name - Should be clear, even and in-line. Embossed cards must have either a cardholder name or description such as 'club member' or 'gift card', etc. For flat-printed cards the cardholder name or description is optional. Check that the title and name on the card match the gender of the person presenting it.
- Expiry date/valid from date - All cards have an expiry date, but only some have a valid from date. Check that the card isn't being presented before its 'valid from' date or after its expiry date
- Contactless indicator - This 'wave' symbol indicates that the card can be used to make payments without swiping it or inserting it into a terminal. This symbol usually appears on the front of the card
- Hologram - These may be on the front or back of the card. The 3D image should move when the card is tilted. If the Visa logo has been placed on the back of the card it will usually be a miniature version. These are the most common holograms currently in use:
  - MasterCard – the world/globe
  - Visa – a dove, which appears to fly

14. Terminology

A

Acquirer – A financial institution that is a member of the Card Schemes and provides facilities for businesses to accept card payments and receive these funds. Also known as a 'card acquirer'.

Address Verification Service (AVS) – Fraud-prevention service that verifies the numerical elements of a customer address against a card.

Authorisation – The process whereby a transaction for a specified amount is approved or declined by a card issuer or an acquirer on behalf of a card issuer. This approval confirms that the card number is valid, that as at the time of

the transaction the card has not been reported lost or stolen and that funds were available. **It does not confirm the authenticity of the card presenter or the card, or guarantee settlement of the transaction.**
The authorisation request may be generated by a customer terminal and processed electronically or may include voice contact between the customer and the acquirer. Find out more about Authorisation and Referrals. See section 5.
Authorisation Call – A telephone call made to obtain authorisation for a transaction.
Authorisation Code – A code (which must not be all zeros) generated by a card issuer or by an acquirer on behalf of a card issuer when an authorisation request is approved.

B
Batch – A collection of transactions held at a single terminal or outlet. A batch may contain any number of shifts or days data.

C
Card Acquirer – See Acquirer.
Card Issuer – The organisation that issues a payment card to the cardholder.
Card Not Present Transactions – Card payments processed when the card and cardholder are not present during a transaction.
Card Number – The long number across the front of a card, also known as the PAN (Primary Account Number).
Card Present Transactions – Card payments processed where both the card and cardholder are present during a transaction.
Card Processing Facility – The agreed products and services provided by BOIPA which allow you to accept and process card payments.
Card Schemes – Visa, MasterCard, American Express.
Card Security Code (CSC) – This is a three-digit code at the end of the signature strip or in a separate white box next to the signature strip on a card. American Express cards have a four-digit CSC on the front of the card. **Never record the CSC – it must only be used for one transaction.** The Card Security Code (CSC) is sometimes also called the Card Verification Value (CVV or CVV2) or Card Verification Code (CVC or CVC2).
Card Testing – When a fraudster places an order over the phone or online to check if the card details they have will be authorised. Find out more in Reducing Fraud. See section 13.
Card Verification Code (CVC or CVC2) – Refer to Card Security Code
Card Verification Value (CVV or CVV2) – Refer to Card Security Code
Cardholder – The person to whom a card is issued, or an individual authorised to use the card. **Cardholder** Authentication – BOIPA Cardholder Authentication is a security tool designed to help you authenticate cardholder details in the online eCommerce environment. It brings together MasterCard SecureCode (SecureCode) and Verified by Visa (VbV) and is also referred to as '3D Secure'.
Cardholder Data – The data obtained as part of a transaction, including:

- PAN / card number
- Cardholder's name
- Expiry date
- Service Code

Cash Back – An optional transaction type where a customer may, with the approval of BOIPA, allow a cardholder to draw cash up to an agreed limit as part of a standard sale transaction. This is also known as 'cash back'.
Chargeback – The term used where a card issuer can reverse part or all of the value of a transaction back to you as a merchant via the acquirer which processed the transaction, for example, when a transaction is disputed because it is proven to be fraudulent or because the customer has not followed the correct procedures.
Chip and PIN – Chip and PIN is a programme aimed at reducing fraud for those transactions where the cardholder and card are present at the time of the transaction. The chip (silver or gold coloured square on the front left side of the card) is embedded into a card to provide highly secure memory and processing capabilities. In addition to holding the same personal data as the magnetic stripe, the chip provides additional security features to safeguard against counterfeiting. The PIN is a four-digit number that the cardholder enters into the PIN pad instead of signing a card receipt. Liability for counterfeit card transactions and lost and stolen card fraud now stands with the party in any transaction who is not chip and PIN compliant. Where all parties are compliant, counterfeit transactions are reduced significantly and there will be no recourse by the cardholder saying they did not authorise the transaction.
'Code 10' Call – A call made to BOIPA Customer Support if you are suspicious about a transaction.
Compromise – Intrusion into computer systems where unauthorised disclosure, modification or destruction of cardholder data is suspected.
Contract – Your formal agreement with BOIPA.

Credit Card – A payment card linked to an account which may be settled in full by a set date or repaid over a period of time, subject to minimum monthly repayments being made. Interest will normally be charged to the cardholder on any outstanding balance. Examples of credit cards include MasterCard and Visa.
Customer Number – The unique number you are given when you sign a contract with us which identifies your business on our systems. This is also known as the Merchant ID (MID).

D
Data Controller - The Information Commissioner's Office website defines this role as:
> "...a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."

Debit card – A card that enables a customer to transfer money from a current account or other similar account to make a payment. Examples of debit cards include Maestro, Debit MasterCard and Visa Debit.

E
eCommerce Transaction – A sale made over the Internet. You need a special agreement with us to handle these transactions.
Encryption – A way of converting information into an unintelligible format that allows storage or transmission of data without compromise.

F
Firewall – Hardware, software, or both that protects data on a network or computer from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.
Floor Limit – An amount agreed between BOIPA and our customer for a single transaction over which authorisation and approval must be obtained. Floor limits above zero are only available for face-to-face chip card transactions. Any transactions over the agreed floor limit will require authorisation to be obtained.

- In most instances floor limits will be set at zero. However, depending on the nature of your business, you may have different floor limits for transactions on your terminal, transactions using paper vouchers and for any card not present transactions. Details of your floor limits can be found in your BOIPA Contract.
- Make sure all your employees know the right floor limit for each type of sale, but do not write floor limits down where customers can see them, or tell customers what they are.
- Your electronic terminal has pre-programmed floor limits and will automatically telephone for authorisation when necessary.
- The floor limit applies even if the cardholder asks to pay part in cash and part by card. If the total amount of the transaction is over your floor limit, telephone for authorisation – even if the card payment amount is below the limit. Tell BOIPA Customer Support that it is a 'split sale'.

M
Mail Order Telephone Order (MOTO) – Transaction where the order and card details are taken over the telephone or by post. Find out more in Mail Order Telephone Order Transactions.
MasterCard SecureCode – see SecureCode.
Merchant ID (MID) – See Customer Number.

P
Payment Card – A generic term for any plastic card – credit, debit, charge and so on – which may be used on its own to pay for goods and services, or to withdraw cash.
Payment Card Industry Data Security Standard (PCI DSS) – A compliance requirement that aims to ensure that cardholder information is always stored, processed and transmitted securely.
Payment Gateway – This is your 'virtual cash till' for eCommerce transactions.
Payment Service Provider (PSP) – PSP's offer retailers online services for accepting eCommerce (internet) payments by a variety of payment methods including cards.
Personal Identification Number (PIN) – A set of digits (usually four) entered by the cardholder to authenticate a chip & PIN transaction.
Primary Account Number (PAN) – The cardholder number of up to 19 digits which is usually, although not always, embossed on the front of the card.

Q
Quick Reference Guide – This is a 1 page double sided reference guide to help merchants with all the key features of their POS device.

R

Reconciliation – The method by which a customer compares the business undertaken at their terminal with that recorded by the acquirer and credited to their bank account.
Recurring Transactions – Transactions that are authorised by a customer to be submitted at regular intervals (i.e., weekly, monthly, quarterly, etc.) and on a predetermined basis.
Referral – When your terminal prompts you to make a manual authorisation call.

S

SecureCode (or MasterCard SecureCode) – A method introduced by MasterCard to provide an additional, secure cardholder verification process prior to an eCommerce transaction proceeding over the Internet.
Split Sale/Transaction –Where a sale is split into two (or more) separate amounts on one (or more) card/s in order to avoid obtaining authorisation for the full amount on one card.

T

Terminal Receipt – The paper receipt that is printed when a transaction is completed.
Terminal User Guide – The instructions that came with your terminal. It is important to read these carefully together with these Customer Operating Instructions.
Transaction – A card payment in exchange for goods or services that you are providing falling within the nature of business you described to us in your application form or which you subsequently notified us of in writing.
Transaction Amount – The full amount the customer pays for the goods or services, including any VAT.
Transaction Data – Information that identifies the purchases a cardholder makes with their card.

V

Verified by Visa (VbV) – A method introduced by Visa to provide a secure cardholder verification process for eCommerce transactions.