THE MORAY COUNCIL

SECURITY GUIDELINES FOR ACCEPTING CREDIT/DEBIT CARD PAYMENTS

Author/s	Frank Kidd		
Version	V1	**By**	FK
Documented on:	February 2016		
Last Review date:	October 2018	**By**	KG

Security Guide

This guide contains some critical information about the procedures associated with accepting credit/debit card payments, and gives details of the steps that you should follow to help raise your awareness of risks and reduce as far as possible, your exposure to these risks.

There are two main environments where payments can be accepted.

Card Present (CHP)

When the cardholder is in front of you and has their card with them at the time of the transaction and you take the payment by reading the chip.

Card Not Present (CNP)

When the cardholder and card are not with you at the time of the transaction. A Cardholder Not Present transaction can take place:

• Over the internet (e-commerce)

• By telephone.

Accepting cards – best practice Card Holder Present

Things to look out for if the card is not accepted by the reader.

Validity dates: The majority of cards will have effective (valid from) and expiry (valid to) dates which are located on the face of the card. The transaction date must fall on or between these dates. Do not accept a card prior to the effective date (the first day of the month) or after the expiry date (up to and including the last day of the month) or you may be subject to a chargeback. Some cards may just have an expiry date. In these cases you'll need to make sure that transactions are not accepted after the last day of the month of expiry.

Cardholder's title: If the cardholder's title is embossed on the front of the card (for example, Mr, Mrs) check that it is appropriate to the person presenting the card. Check that there is no obvious discrepancy between the cardholder and the card. For example do they look to young to have a card?

Cardholder's signature: The signature strip should not be disfigured or tampered with in any way and should have only one signature. If you are presented with an unsigned card do not allow the cardholder to sign the card until the cardholder has successfully entered the PIN, they should be advised to sign the card.

Bank Identification Number (BIN): On Visa and MasterCard cards check that the first four digits of the card number are printed in small characters below the first four digits of the card number. If the four digits are missing or do not match, the card is probably counterfeit.

Damaged cards: Ensure that the chip on the card you are presented with has not been mutilated or damaged in any way.

Accepting cards – best practice Cardholder Not Present

Ascertain that the person on the other end of the phone is the cardholder and not using someone else's card. If they are using someone else's card ask if the cardholder is present and speak to them. If not politely decline the request and explain that it has to be the cardholder giving the details.

Make sure that the card is valid and in date.

If payment goes through ask if they would like the transaction number as reference for payment or we can e-mail the receipt to them.

Verifying cardholders using chip and PIN

When a card with a chip is inserted into the chip card reader, the processing equipment will ask the cardholder to enter their PIN (personal identification Number) to confirm the transaction. The processing equipment will ask for authorisation for all chip-and-PIN transactions.
If authorisation is declined, do not go ahead with the transaction as we will not be able to defend you if the transaction is charged back at a later date. Ask the Customer for another method of payment. Do not swipe the card or enter the details using the keys on the device.

What information must be securely stored?

On completion of a payment any receipts printed must be stored in a secure environment i.e. safe, lockable cabinet or approved container. Any secure container where receipts are retained should be restricted to only officers with operational/management requirements.

Merchant copy receipts should only be kept for a period of 6 weeks.

Any information that is necessary to process card transactions correctly, including any information which is recorded electronically or otherwise on any payment card. Destroy after six weeks.

Any information that is used to authenticate a card payment, including the card number, expiry date, issue number, passwords, pass phrases and any other unique information supplied as part of the card payment. Destroy after six weeks.

Any information that could identify individual cardholders and their purchases. This includes name, address, description of the purchase, amount and other details of the card payment. Destroy after six weeks.

Additional Security Considerations

A list of all staff eligible to take card payments is to be maintained for each Service location and any changes or amendments are to be notified to Payments Section immediately by the Service location manager.

The physical location of the chip and PIN terminal and security of its parts should be considered. Can it be removed easily? Are the separate parts physically protected to prevent tampering or theft?

Chip and PIN terminals should always be placed in a location that allows the cardholder to use them in a way that prevents other cardholders from seeing the PIN.

Where practical, terminals should include PIN shielding.

Officers should check the condition of chip and PIN equipment on a regular basis to ensure that it has not been tampered with. Checks should include an inspection of the cabling to ensure that nothing has been added.

Only authorised personnel should be allowed access to chip and PIN equipment. Officers should not allow access to machines by Engineers without prior authorisation and notification. This notification/authorisation should be done through the Service Manager. Always ask for identification and be very suspicious of any engineers turning up without prior arrangement.

Security training should be carried out to remind staff of their responsibilities at least annually (and more regularly where staff turnover is high). This training should be an integral part of the induction of new staff. Staff access to sensitive data should be managed accordingly. This includes staff who have no operational responsibility but have physical access to buildings (for example, staff not directly employed by your organisation – such as cleaning and maintenance staff).

When employees leave the employment of an organisation it is important to ensure that all of their access rights and security related entitlements are revoked. In particular ensure that all keys are returned and that any physical access codes are changed so that they cannot subsequently enter secured areas.

Whilst the above is the minimum criteria from a security point of view, it is agreed that each individual Service should have individual guidelines and procedures relevant to their own area. Managers should review these procedures at least once a year and provide a copy of their procedures to Payments Manager. Managers

should also ensure that their staff read and sign annually as having read and understood these instructions.

PCI Compliance

Payment Card Industry Data Security Standards

What is PCI DSS? › What is PCI DSS?

Payment Card Industry Data Security Standards were introduced to:

- Provide global data security mandate introduced by the card schemes - both physically and technically
- Enhance cardholder security
- Give the customer confidence

PCI DSS applies to every organisation and retailer that deals with card payments and transactions. Compliance with PCID DSS is mandatory for all merchants.

Payment Card Industry Data Security Standards

What is PCI DSS? › How do we comply?

We can comply by:

- Protect stored cardholder data
- Fire walls, encryption of data transmission
- Information Security Policy
- Monitor and test IT networks
- Annual assessment of compliance
- Staff awareness

Failure to comply could result in fines up to £50,000 per infringement.

Payment Card Industry Data Security Standards

Payment Card

Primary Account Number (PAN)

Card Security Code (CSC) or Card Verification Value (CVV2)

Personal Identification Number (PIN)

Cardholder not present transactions (CNP)

Payment card: Credit or debit card issued by Visa, MasterCard or another card provider

Primary Account Number (PAN): The unique payment card number (usually 14-16 digit number on the front of the card) that identifies the issue and the cardholders account. Sometimes known as the 'long' card number.

Card Security Code (CSC) also known as the Card Verification Code (CVC): The three or four digit number printed on the payment card that securely ties the PAN to the plastic card.

Personal Identification Number (PIN): The numeric password (usually 4 digits) known only to the user and system to authenticate a transaction. The user is only granted access if the Pin the user provided matches the PIN known to the system

See if you can answer the following:

What does PCI DSS stand for?

- ◯ Payment Card Industry Data Security Standards
- ◯ Personal Credit Industry Data Security Standards
- ◯ Payment Credit Industry Data Standard Security
- ◯ Payment Card Industry Data Standard Security

Is this statement true or false?

"PCI DSS applies only to Public Sector organisations that deal with card payments and transactions."

- ◯ True
- ◯ False

Is this statement true or false?

"It is impossible to access the authentication data held in the chip or magnetic strip on a card."

- ◯ True
- ◯ False

Which of the following can result when card details are lost?

- ◯ Negative media
- ◯ Loss of customer confidence
- ◯ Fine and penalties for non-compliance
- ◯ Termination of payments by card

Which of the following is correct?

Failure to comply could result in fines up to...

- ◯ £5,000
- ◯ £500,000
- ◯ £50,000

PAN is the term used to describe which of the following?

- ◯ The validation code on the reverse of the card
- ◯ Any credit or debit card issued by MasterCard
- ◯ The number that identifies the cardholders account
- ◯ A transaction when the card holder is not present

Which of the following can legally be stored following the transaction?

- ◯ Name
- ◯ Security number
- ◯ PIN number
- ◯ Expiry date

Complete the following statement:

I can help to protect card data by:

- ◯ Emailing customers details and card numbers to an employee
- ◯ Repeating card numbers back to the customer over the phone
- ◯ Recording customers card details on an excel spreadsheet
- ◯ Asking the customer to email their card details to me
- ◯ Using only the authority approved payment service programme to process transactions

Which of the following services and individuals are responsible for maintaining the security of cardholder data?

- ◯ Finance
- ◯ ICT
- ◯ Cardholder
- ◯ All staff involved in transaction processing
- ◯ The bank

What does CSC stand for?

- ◯ Card Security Code
- ◯ Card Standards Corporation
- ◯ Clever Security Codes

Is this statement true or false?

"I can ask the customer for their PIN number if there are problems processing the payment/transaction?

- ◯ True
- ◯ False

To ensure that all staff are aware of the security aspects of accepting card payments it is advised that all Managers should ask that their staff read and sign as having understood the above and carry this out Annually.

In order for The Moray Council to remain PCI DSS Compliant we are required to have in place a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. The defined retention timescales are 6 weeks. An e-mail reminder to all Managers/Users will be sent out quarterly to remind them and their staff to destroy all out of date Debit/Credit Card Receipt slips.