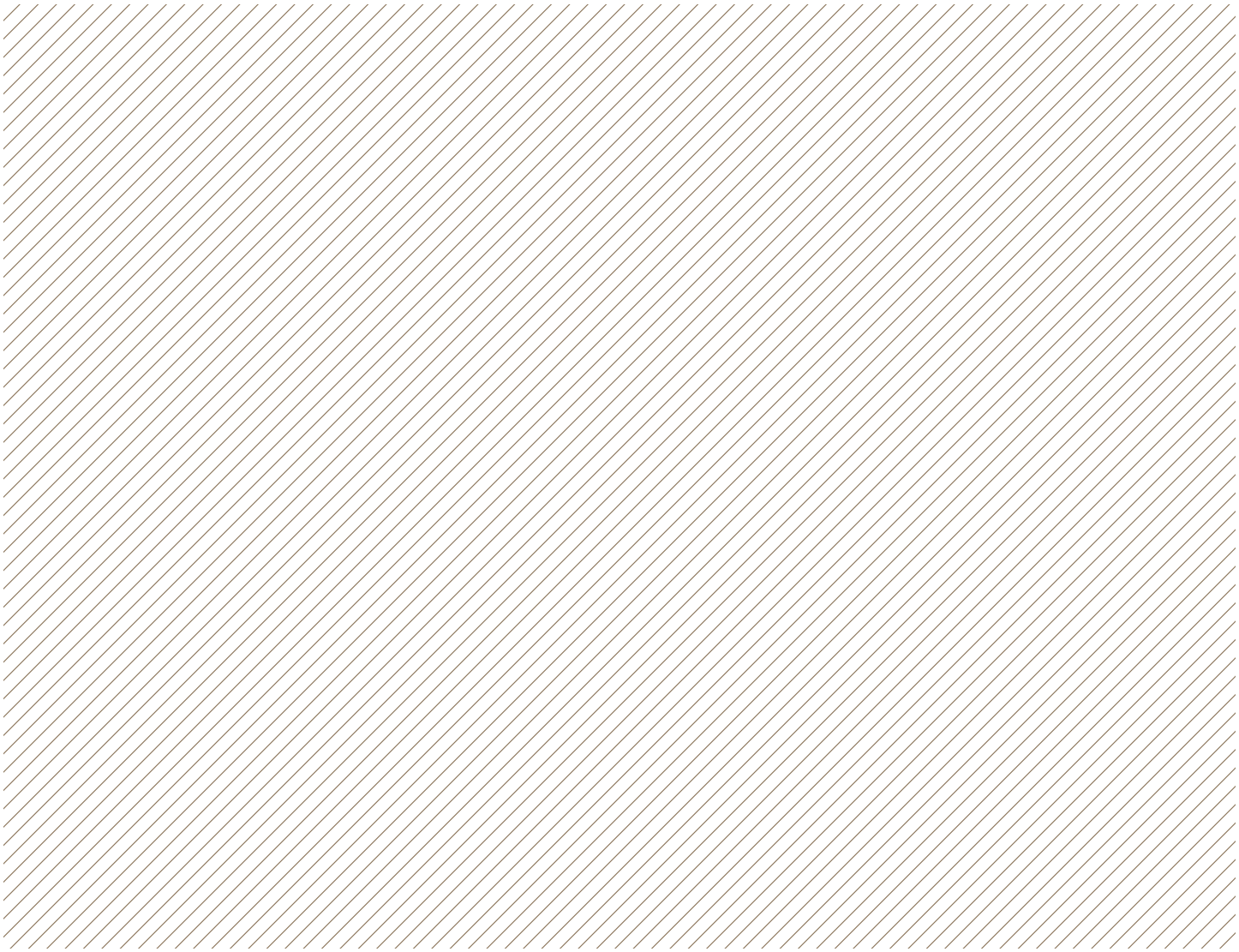
In partnership with

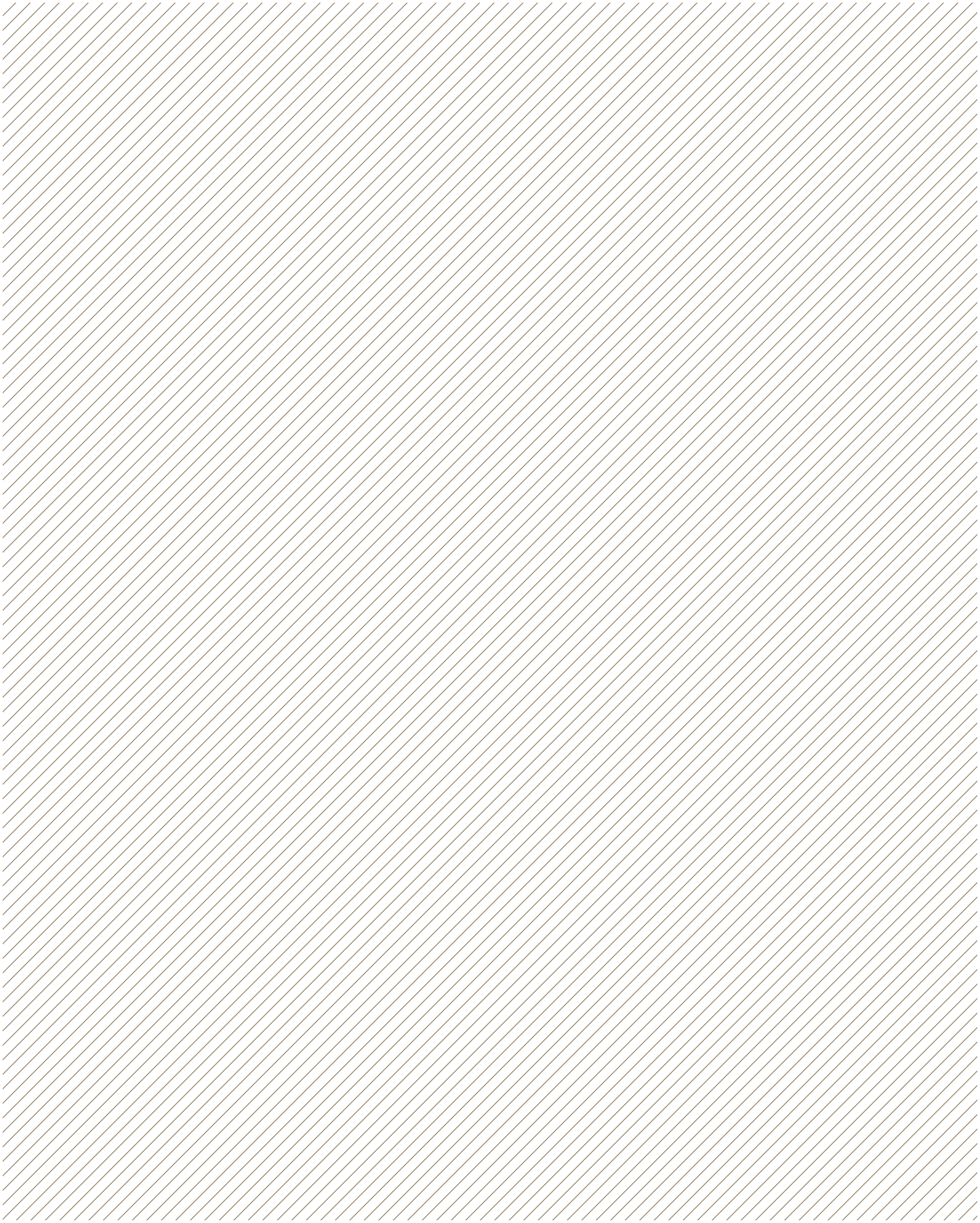
Financial Fraud Action UK
Working together to prevent fraud

THE UKCARDS ASSOCIATION

Security guidance for card acceptance devices

Deployed in the face-to-face environment





The UK Cards Association is the leading trade association for the cards industry in the UK. With a membership that includes all major credit, debit and charge card issuers, and card acquiring banks, the role of the Association is both to unify and represent the UK card payments industry. It is responsible for formulating and implementing policy on non-competitive aspects of card payments including codes of practice, card fraud prevention, major infrastructural changes, development of standards and other matters where cross-industry benefits are identified. The UK Cards Association was formed in April 2009 as the successor body to the APACS Card Payments Group.

Contents

1 Introduction

The card payment industry is continually subjected to sophisticated attacks by fraudsters designed to gain access to sensitive card data and confidential PINs. The level of sophistication and the amount of effort fraudsters are prepared to put into defeating the security measures continues to increase. This requires the industry to provide, as a complement to its multi-layered approach to information security, guidance to stakeholders in reminding them of their responsibilities in securing card payments.

Chip and PIN is proving highly successful in defeating certain malicious attack types. Within the UK there are now in excess of a million chip and PIN terminals and PIN entry devices. The UK industry continues to be proactive in seeking methods to improve the industry's defence against attack and the provision of good practice guidance helps all involved to defend card payments against the real threat of financial loss and reputational damage.

This guideline is intended to be used by retailers accepting or intending to accept face-to-face card payments and is designed to complement card industry rules and regulations and advice given by point-of-sale solution providers (including banks and third party suppliers). The advice and guidance offered should be considered when reviewing or developing security procedures and processes for the point-of-sale environment, particularly, but not exclusively, those relating to the acceptance of card-based transactions.

In providing general advice and guidance we recognise that a one-size fits all approach is inappropriate and that allowance must be made for the wide variation in point-of-sale configurations and also the level of resource available to be put into security measures. The purpose of this document is to assist understanding of the financial and reputational implications of the theft of assets, re-introduction of fraudulent assets back into the live environment and the detection of any fraudulent assets.

To assist particular market environments we have included a small number of case studies (on pages 6 and 16) to illustrate issues that have been identified during consultations with other trade bodies and interest groups.

1.1 Intended audience

The intended audience for this document is the manager or management team within a company that is responsible for the security of retail premises and the assets within those premises like PCs and point-of-sale and CCTV equipment. Some of the content is of a technical nature and if in any doubt retailers should contact their acquiring bank who will be able to assist them in maintaining an effective level of security for card payments and the associated equipment.

1.2 Management summary

The ultimate responsibility for the protection of cardholder data, within a retailer's equipment, lies with the retailer and they have to ensure that only correctly certified and evaluated equipment is sourced from reputable vendors. Additionally, having made the right selection, the retailer must protect that asset from being used fraudulently; the purpose of this document is to assist retailers in doing that.

Retailers must be aware that the chip and PIN devices on their premises are valuable assets that, if not protected throughout their complete life cycle, could be compromised by criminals and used to perpetrate fraud that will ultimately have a financial impact on the retailer and may also cause reputational damage that may further adversely affect business.

The need to secure devices begins from the moment they are released from the vendor to the retailer and the tracking of that asset, once delivered, becomes the responsibility of the owner (acquirer, third party provider or retailer) wherever it is stored, whenever it is in transit and wherever it is installed.

This document covers the threats (electrical, electronic and physical) to chip and PIN devices and the actions that can be taken to mitigate these threats.

In order to place the guidance that follows into the right context it is important that the reader understands which assets require protection and the potential consequences of a compromise of these assets:

- Cardholder Data and Card Data including the PIN;
- PIN Entry Device (PED) / Terminal throughout its life cycle;
- Software resident in PEDs, terminals, EPoS systems and retailer's servers and central computers;
- Retailers', vendors' and card processors' reputations

2 Assets and threats

2.1 Physical assets

In the case of face-to-face card transactions the principal assets under threat are the personal payment card details and personal identification numbers (PINs) used to verify the cardholder's identity.

Personal payment card details – referred to as sensitive cardholder information in the Payment Card Industry Data Security Standard (PCIDSS) – include the primary account number, start and expiry dates, service code and the CVV (card verification value). Currently these values can be obtained from the magnetic stripe on a live card and from the static data embedded in the integrated circuit of a chip card. This information is at risk when it is captured from the card in a reader or in the data messages passed to and from the point-of-sale. It is possible for fraudsters to use the data that can be captured in a live transaction to create a plausible magnetic stripe clone of the live card.

With the advent of chip and PIN, personal payment card data alone is of limited value for face-to-face transactions in the UK unless the associated PIN can be obtained. However, the information, including the PIN is still valuable to fraudsters, particularly for use overseas and the industry has seen an increasing level of sophistication applied to the capture of these assets, either directly from the keypad of a PIN Entry Device or through recording the transaction using hidden micro-cameras. Fraudsters have successfully deployed examples of both attack methods.

Criminals then use the captured card details along with the PIN to manufacture cloned magnetic stripe cards that are then used to withdraw cash from cash machines or at the point-of-sale in countries that have not yet upgraded to chip and PIN.

2.2 Reputational assets

Whilst this fraud is not directed at the retail community any consequential loss of confidence in the overall security of card payments does represent a business risk. Any association with the compromise of card information is potentially damaging to the retailer from a reputational and brand value point of view.

If a significant breach of security is identified that can be directly attributed to the bad practice or failure to comply with required regulations by any party in the card payment process then it will result in reputational damage. This may have additional significant effects on their business in, for example, costly accelerated implementations to reach compliance or litigation costs.

2.3 Financial Loss

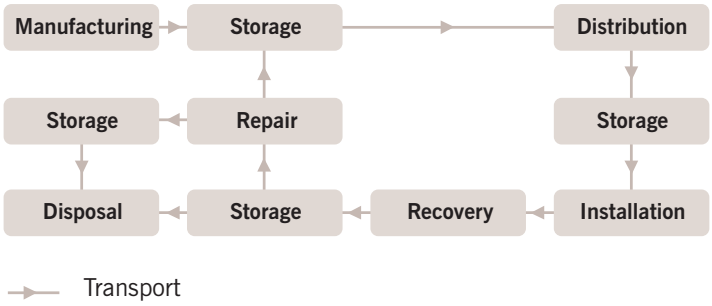
Increasingly the international payment schemes look to impose fines and penalties on those parties held liable for the compromise or loss of sensitive data. The level of such fines are such that they may threaten the financial security of the organisation.

Retailers who own their own point-of-sale devices should realise that if these are compromised and devices need to be replaced they will incur the additional cost.

2.4 Threats

To combat threats to these assets it is necessary to consider the whole life cycle of physical devices (PED/ Terminals) from the point of manufacture through to the point they are destroyed – see Figure 1. Device Life Cycle below.

Figure 1. Device Life Cycle



Much of the life cycle is also applicable to the retailer's own system software or payment applications purchased from software vendors.

To be able to perpetrate many of the threats and attacks described in the following sections the fraudster has to compromise one of the elements of the life cycle. Whilst technology may assist in combating some threats, vulnerabilities are greatly reduced by robust processes and procedures. All parties should treat their assets as high value items.

Listed below are some of the principle attack methods currently deployed against the card acceptance environment for the purposes of capturing personal payment card details and PINs. The list is used to provide real examples of the types of attack seen in the card payments space and to illustrate the range of security measures that are required to secure the environment.

2.4.1 Electronic attacks

Electronic attack is used here as a general term to cover a range of logical attacks carried out against point-of-sale devices and systems that capture and process card transactional data. The listing in itself is not exhaustive and it should be understood that with new advancements in technology come new potential attack methodologies.

2.4.1.1 Hacking

Hacking is a direct attack against systems and sources to gain access rights that would lead directly to the compromise of sensitive data as it is being processed. More typically such attacks are directed against the operating systems (such as Microsoft Windows) on the computers running point-of-sale applications but more recently the use of internet-based services has provided a further avenue of attack for fraudsters.

The recent deployment of wireless technology in the retail environment is of considerable concern as a potential new area of vulnerability. Incidents of card data being captured over radio connections have been the source of considerable fraud in the United States. Retailers should ensure that messages sent over radio connections are suitably encrypted as described in UK Cards – Card Acceptor to Acquirer Interface Standards – Standard 70.

2.4.1.2 Rogue or malicious software

Illicit software can be loaded into the point-of-sale system with the purpose of capturing or re-directing sensitive data that can be retrieved by the fraudster. The use of third parties to provide point-of-sale services and equipment provides an opportunity for unauthorised software to be loaded without the knowledge of the retailer; careful consideration should be given to granting remote access to outsourced service providers.

2.4.1.3 Data logging

This is the ability to capture data as it is passed between components of a point-of-sale system and is often achieved by the insertion of a bugging device. In recent cases the industry has seen examples of such devices being inserted in order to capture card data from the magnetic stripe reader and also to record the key depressions from the PIN pad See Pic 1.

2.4.1.4 Eavesdropping

This is the electronic monitoring of data messages from wireless devices or the monitoring of the electro-magnetic radiation from components of a point-of-sale device to reveal sensitive data. For example – messages from a wireless PoS device may be intercepted and must therefore be secured as defined in UK Cards – Card Acceptor to Acquirer Interface Standards – Standard 70.

2.4.1.5 Wiretapping

The tapping of phone lines could expose data and the industry is aware of a number of instances at home and abroad where dial-up connections have been 'bugged' and card data captured. Retailers should ensure that all communications equipment and wiring in their premises is only accessed by authorised staff.

2.4.1.6 Pinhole cameras

In some attacks criminals are using pinhole cameras to record and relay images of PINs entered by cardholders. These cameras are either placed in a strategic position within the store or in some cases attached to a point-of-sale device. Pics 2 and 3.

1. Data logger

2. Downward-facing camera

3.Pinhole camera in ceiling tile

2.4.2 Substitution attack

The attacker is able to remove legitimate components of the point-of-sale device or solution and substitute them with compromised or bogus devices that can illegitimately capture card data or PINs. In some cases the complete device may be removed and a substitute provided. In many cases the bogus device will be exactly the same as the device removed.

Criminals have used a variety of methods to substitute devices, ranging from the bogus service engineer turning up to swap out allegedly faulty devices to the threatened use of violence.

2.4.3 Theft

The attacker removes point-of-sale equipment with the aim of gaining access to any stored data that may be held within the device.

Devices are often stolen with the intent to reverse engineer them and to learn about the security controls incorporated in them. This often leads to the introduction of additional components designed to compromise the device and these are re-introduced into the live environment. This is often the first step in a chain of substitution attacks.

2.4.4 Targeting of redundant equipment

Where redundant equipment is disposed of or sold on without ensuring that any stored data is deleted from the device they become a primary target for the criminal wishing to harvest any data that may be present. Devices may also be sought with the intent to add bogus components and to re-introduce them back into the live environment.

2.4.5 Members of staff

It is not unheard of for criminals to take employment to enable them to perpetrate any one or more of the above attacks or to compromise or corrupt members of staff to act on their behalf. Merchants must consider what measures need to be in place to protect staff from such threats and in particular for those staff deemed to be high risk, for example staff working extended hours for minimum wage or staff left on site alone.

The insider threat is well recognised and merchants must assess the level of threat their own members of staff represent and restrict access to sensitive data or functions accordingly. Consideration should also be given to staff who have no operational responsibility but have physical access to buildings, such as cleaning and maintenance staff. Finally, it is not just a retailer's own staff that need to be considered but also staff employed by outsourced service providers and in particular those with access to systems that process or store cardholder information.

2.4.5.1 Malicious insiders

Any insider with malicious intent can severely compromise cardholder information. They can range from the disgruntled employee to members of staff who have been corrupted or compromised by criminals and to criminals who have taken employment to position themselves to be able to perpetrate any one or more of the attacks described in this guide.

2.4.5.2 Curious users

Increasingly merchants employ highly qualified individuals in what may be seen as junior or routine positions. This includes people with a high degree of technical expertise. Such staff may be tempted to explore the boundaries of the systems they are enabled to use and this curiosity may lead to the abuse of access rights.

2.4.5.3 Poorly trained staff

Staff that are poorly trained represent a threat if they do not follow correct processes and procedures. Such weaknesses may be exploited by criminals to carry out fraud or compromise card data. Simple things like allowing unauthorised access to point-of-sale equipment may result in sensitive data being compromised. (See Case Study 1 - Referral Transactions.)

2.4.6 Security controls

Criminals will seek to test any of the security controls in place to defend against attack and the more they can learn about a particular set of controls the easier it may become for them to defeat them and obtain sensitive card data. It is important therefore to ensure that details of the controls in place are kept confidential.

Organised criminals have sufficient resource and expertise to spend considerable time and effort to defeat security controls and they carry out much of the card fraud seen in the UK. It may be prudent to assume that criminals are familiar with the design of most systems and, therefore, retailers should protect their systems with this assumption in mind.

2.4.7 Support and maintenance

Where third party suppliers (that may include manufacturers of components) support point-of-sale systems it is important to guard against attack through this channel and for there to be a process of authorising changes to devices or systems that support card payments. Access, by a third party, to point-of-sale equipment to make changes must be controlled. (See Case Study 2 - The Bogus Engineer.)

Case Study 1 – Referral Transactions

Occasionally authorisation requests will result in the transaction being referred to the issuer - usually for higher value transactions, where additional security checks are needed before the transaction is authorised. Criminals have found that in some cases, where the point-of-sale device is handed to the customer for PIN entry, they are able to manipulate the device into believing that the referral has been carried out successfully. If, through poor understanding of the correct procedures, the operator fails to spot the terminal instructions on their side - and the transaction is completed without the necessary intervention - the merchant will lose both the goods dispensed and receive a chargeback for an unauthorised transaction.

Terminal vendors have introduced an additional step into the process that requires a supervisor card to be swiped before a referral transaction can be completed. Merchants should ensure that this additional step is implemented on their equipment and ensure that staff read and check the merchant-side screen messages at all times.

Case Study 2 – The Bogus Engineer

There have been numerous cases where a compromised PED has been installed in a merchant location by an apparently legitimate technical support engineer. Fraudsters will even go to the lengths of sourcing uniforms and fake identity cards to appear legitimate.

It is good practice to ensure that no-one is given access to point-of-sale equipment unless they are expected and their ID can be verified. Firstly, ensure that you book the appointment at a time convenient to you, and when a manager or supervisor can be present to check the credentials of the engineer. If possible get the name of the individual booked to attend and check with the support company if someone else arrives.

3 Consequences of compromise

3.1 Fraudulent use of card data

The data captured by compromised devices tends to be exported from the UK to countries where chip and PIN has not been introduced. This enables the captured data to be encoded onto the magnetic stripe of cards and for these cards to be used fraudulently at both point-of-sale and to withdraw funds at cash machines.

The data may also be used for card-not-present (CNP) fraud that is now the biggest card-related fraud in the UK, and the USA.

3.2 Damage to the card industry

The card industry would suffer direct financial costs if there were a major card compromise at a retail point-of-sale, using compromised PEDs, both through fraud and then potentially through the necessity to conduct a forced card re-issue to replace cards that had been compromised. This would be a significant cost to the industry, as well as damaging the credibility of card products and payments within the UK.

Additionally, the publicity around any major compromise of a retailer's equipment could damage consumer confidence in card payments in general and chip and PIN at the point-of-sale in particular.

3.3 Damage to the retailer or brand reputation

A major card compromise at a retail point-of-sale, using compromised PEDs, could lead to a loss in customers as some would lose confidence in the retailer's ability to trade safely and for larger retailers this could have a knock-on effect on their whole brand.

Retailers should be aware that they may be held liable for any fraud should it be proved that the compromise of data was the result of negligence. The financial penalty may be significant and threaten the long-term profitability of an organisation.

3.4 Damage to the vendor or brand reputation

A major card compromise of any vendor's equipment or software applications could seriously impact their future sales as potential customers may doubt the vendor's ability to provide secure products. This could have a detrimental effect on the vendor's brand.

4 POS & EPOS terminal components

For the purpose of accepting payment card based transactions, point-of-sale devices are made up of the following functional units:

- The interface device (IFD): the unit that a payment card is inserted into in order to read the personal card data. This may take the form of a magnetic stripe reader or an IC card reader;
- The PIN entry device (PED): the unit with a keypad, that is primarily used to prompt the cardholder to enter their PIN;
- The terminal or point-of-sale (POS): the unit that communicates with the other components and controls the process of card acceptance;
- Electronic point-of-sale systems (EPoS): the unit that communicates with the other components and controls the process of card acceptance in an integrated environment.

These units can be combined in a variety of different ways and may or may not be integrated into the merchant's own point-of-sale equipment and systems.

In today's point-of-sale environment, the device manufacturer or third party normally manages acceptance devices through a Terminal Management System (TMS). This is used to control the software driving the various components, the parameters used to manage card acceptance and for security key management. Retailers are encouraged to work closely with and seek guidance from their acquiring bank who should have specialists with the in-depth knowledge to advise on these issues.

4.1 General security requirements

By only buying approved devices and components retailers can ensure that they comply with the minimum security requirements for point-of-sale devices as laid down by the card payment schemes through PCI Co., the banking industry and, for functional security, EMV Co. These can be summarised as follows:

4.1.1 Tamper evident/Tamper responsive

For the benefit of the cardholder, point-of-sale devices should at least be tamper evident, in that it should be obvious to the customer when an attempt has been made to defeat the security features of the device.

In the case of the PIN Entry Device the requirement is for the device to be Tamper Responsive, in that any attempt to defeat the security feature shall result in the immediate erasure of all sensitive data, such as cryptographic keys or PIN values and the device shall cease to function.

Where components of an acceptance device are combined, for example where the IFD, PED and terminal are one and the same, the requirement is for the whole to be tamper responsive.

4.1.1.1 Device certification

It is a UK acquirer requirement that all PEDs deployed in the UK be evaluated to an Assurance Level of EAL4+ under the Common Criteria[1] methodology and against PED Protection Profile Version 1.37. Devices evaluated to this level have been proven, through a robust and independent evaluation process, to meet the security requirements of the UK card payments industry.

For global interoperability it is also a requirement that PEDs be evaluated under the Payment Card Industry (PCI) PoS PED process. PEDs may not be deployed if they have not passed these evaluations. Your chosen manufacturer should be asked to provide assurance and evidence that they comply with the above standards.

4.1.2 Cryptographic requirements

To support IC card acceptance, devices are required to carry out cryptographic functions as part of the transaction process and in order to protect sensitive data as it is transferred from one component to another. Requirements in this area are well documented in industry standards and specifications and retailers should ensure that all devices deployed have passed the appropriate security evaluations. This may be in the form of a certificate or letter of compliance supplied by the vendor, or the retailer may consult the PCI and banking industry websites for the appropriate notifications. Where the device is supplied by the acquiring bank or a third party processor it is their responsibility to ensure the compliance of the devices they deploy.

Websites:

- PCI website for a list of PCI-approved PED devices - https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html
- The UK Cards Association web site for Common Criteria evaluated devices - http://www.theukcardsassociation.org.uk/about_us/what_we_do/technical_services_and_standards/common_criteria_evaluation/-/page/477/

4.1.3 Physical security

Consideration must be given to the physical protection of point-of-sale devices particularly where components are physically separated. All connections should be physically secure, for example, it should not be possible to simply detach a PED from its terminal by pulling the wire out. Where possible, connections should be hard-wired and only authorised maintenance or supervisory staff should be able to swap-out components.

Protection of the point-of-sale device and its components should be considered when locating the device and the following sections provide guidance on the operational environment.

4.1.4 Logical security

It is essential that the card payment application and in particular the EMV software kernel, is logically separated from any other application running on the point-of-sale device. Access to the application must be restricted to ensure its integrity.

Where components are separate each element should authenticate itself to the terminal. This may take the form of a regular 'heartbeat' check. It is recommended that the heartbeat checks are carried out at least every twenty-four hours, preferably every eight hours and more frequently if possible. All events should be logged and negative events (such as missing heartbeats or incorrect handshakes) alerted for supervisor attention.

4.1.5 IP-based/Wireless communications

MasterCard has specified security requirements for point-of-sale solutions that communicate using IP-based or wireless protocols. Details of these requirements and the associated compliance programme can be obtained from your acquirer or direct from MasterCard. UK Cards – Card Acceptor to Acquirer Interface Standards – Standard 70 define the UK requirements.

1. The Common Criteria is a Government approved robust, independent security evaluation process designed to ensure that products meet security requirements set out in a Protection Profile. Varying Evaluation Assurance Levels (EAL) exist within the process, EAL4+ being chosen for PEDs based on the threat environment that exists in the UK

5 General security

The security of the payment process must be dealt with holistically; simply deploying an approved PED with no controls over who has access to stock or installed equipment will break the chain of asset management. It is necessary to raise the awareness of the intrinsic value of these devices and prevent them being treated as worthless throw away items.

5.1 Operational environments

Regardless of the security features built into point-of-sale equipment it is essential that the operational environment they are deployed in is physically secure and that the devices are subject to good management throughout their lifecycle (see Figure 1. Device Life Cycle). Devices are also vulnerable at any point where they are stored and whilst in transit.

5.1.1 Point-of-sale environments

It is recognised that the point-of-sale environment can vary vastly from one retailer to the next and it is impossible to define a single set of requirements that will satisfy all. For example the requirements to secure attended devices are vastly different for those for an unattended device.

With this in mind the following general considerations must be taken into account when placing devices.

5.2 Physical security

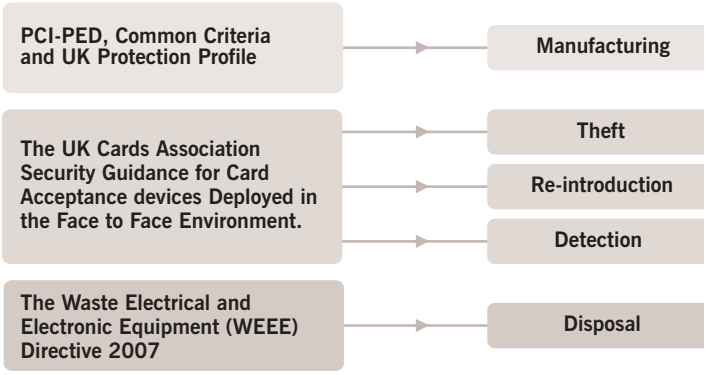
The physical security of assets begins with the manufacturing process and this is defined by the PCI-PED requirements and by the UK Protection Profile that is built upon the Common Criteria. This document covers the vulnerabilities after manufacture, the theft of assets, the re-introduction of rogue assets or modified stolen assets and the detection of introduced assets.

As shown in Figure 2. Zones of Defence, effective application of technology processes and procedures at each level should reduce the effort required at lower levels. By only deploying assets that are approved reduces the vulnerability to attacks and therefore their desirability to criminals. Taking measures to reduce the potential for the theft of devices limits the pool of devices available for criminals to modify. Robust processes and procedures at store level and controlling access to equipment reduces the ability of criminals to introduce devices into the payment process. Finally, effective detection and reporting of attacks to the payment process allows all parties to learn and continually improve all layers of the model.

5.2.1 PIN protection and shrouds

To assist cardholders in protecting their PIN entry from being seen either by 'shoulder-surfing' or by pinhole cameras, some point-of-sale or PED mountings are fitted with in-built or additional shrouds. Care must be taken in selecting these items as they may have a detrimental effect on disability compliance and in some cases may invalidate PED approvals. It is recommended that specific guidance is sought from the acquirer before any shroud devices are purchased and fitted.

Figure 2. Zones of Defence



5.3 Theft of PEDs and terminals

To be able to introduce compromised devices into the point-of-sale environment criminals first have to obtain source devices to modify. There is a need, therefore, to make every reasonable effort to prevent devices being stolen not only to prevent their compromise and re-introduction but also because the asset will have to be replaced at the retailer's expense.

5.3.1 Securing devices in storage and transit

5.3.1.1 Storage of devices

Spare devices are often left at store level to effect an immediate swap-out of faulty devices. Lack of staff education and device management can lead to devices being left on the office floor for days or weeks, and these offer a prime target for theft. If devices are kept at store level then staff should be educated to treat them as they would cash or books of postage stamps and not leave them lying about but have them locked

away securely. Faulty devices should be collected for return for repair at the earliest opportunity and the faulty device managed no less securely than a working unit.

Where replacement units are held centrally consideration should be given to using third party 'caged' secure storage where device serial numbers and the asset register can be handled more effectively.

5.3.1.2 Transport of devices

It is key that owners of devices maintain an end-to-end visibility of their devices throughout their life cycle including the tracking of devices during any transport phase. This can include a number of stages:

5.3.1.3 Device collection from storage

Where devices are held centrally ensure that the person collecting the device is entitled to do so, whether engineer or courier. The PED device should be released and logged as despatched, together with the logging of the serial number and any other specific identification required of who collected the device.

5.3.1.4 Device delivery to site

This could include a pre-issued security code that needs to be verified by the courier/carrier prior to the PED device being released, swapped or collected. This code could be a barcode emailed to the delivery point that can be scanned by the courier/carrier prior to the device being released. The collection of such data could be recorded for future reference, audit and compliance.

5.3.1.5 Site notification

Consideration should be given to telephone, SMS or email notification, prior to delivery of a replacement device, so they are aware of a pending delivery, swap or collection together with the necessary instructions and security procedures. This will make the bogus engineer 'just turning up on site' approach to re-introduction more difficult.

5.3.1.6 Device collection

Swapping devices is inherently a danger area for fraud. The delivery process should ensure that a new product is not released to a site unless a returned product/part is supplied. This should combat a bogus member of staff taking delivery of a new device that will be diverted elsewhere. This should also ensure that PED devices do not remain in a dangerous state of limbo, neither in service nor in safe storage.

5.3.2 Securing the device once installed

In considering the prevention of theft, once the device is installed, it is necessary to strike a balance between securing the asset and damaging usability and therefore, customer service. It may be possible to attach the device in such a way that prevents it being snatched but this will not necessarily deter the bogus engineer or collusive member of staff.

Therefore the physical location of the device and security of components should be considered. Can it be removed easily; are components hard wired together or physically protected to prevent easy tampering or theft? Devices should always be placed in a location that allows the customer to use them in a manner that obscures their PIN entry from other customers and where practical should include PIN shielding. Secure cradles should be used to minimise opportunities for theft but care must be taken to balance security needs with the requirements of the Disability Discrimination Act 1995.

Where the needs of the Disability Discrimination Act can be met with the device in a mounting bracket, consideration should be given to modifying the bracket from a 'support-only' mechanism to one that physically restrains the device reducing the potential for a 'smash and grab' type theft. Where locking the device into the mounting bracket would contravene the Disability Discrimination Act, consideration should be given to connecting a security wire cable to the device and the mounting bracket so giving a degree of movement but maintaining security against a snatch theft.

If you believe that your POS device is vulnerable to theft then there are service cradles and secure harnesses and tethers available to purchase commercially.It may be worthwhile considering their use.

5.3.3 Members of staff

Customer-facing staff have an important role to play in the prevention of the theft of devices but it should be recognised this is not their primary role and their vigilance may not be consistent. In accordance with safe recruitment policies and procedures, a standardised recruitment and vetting procedure should be adopted covering all employees (whether full, part time, temporary, or contract). This procedure should also cover security staff whether external or internal and all IT staff.

Employee application processes should include verification of employees' past history and work record as far as allowed by law.

It is good practice to develop a documented security policy that is available to all staff and where possible allocate personal responsibility for security matters to a manager, who can act as a point of contact for staff on security issues.

At least annually and more regularly where staff turnover is high, security training should be carried out to remind staff of requirements. Security training should be an integral part of the induction of new staff.

In addition it is essential that staff be made aware of all the potential attack methodologies described in this paper and encouraged to report any issues or concerns they may have. This should be to a designated member of the management team or if they are not available, or if the member of staff wishes to remain anonymous because they believe colleagues may be involved, then Crimestoppers can be contacted.

Contact details are:
www.crimestoppers-uk.org or call 0800 555 111

It is good practice for security-related activities, such as swapping out faulty point-of-sale equipment, to be carried out under dual control.

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

It must be recognised that staff can be a vulnerability:

- bogus engineers can dupe members of staff with plausible information to gain access to stores and equipment
- staff can be corrupted to facilitate criminal activities
- staff can help facilitate criminal activities through extortion
- staff can be sympathetic to the organisation sponsoring the criminal activities.

Because of the 'human element' it is very difficult to completely close down the ability of criminals to obtain devices and in some cases the devices are simply snatched from the point-of-sale by petty criminals to sell on. Using some of the methods described in section 5.3.1 – Securing devices in storage and transit – these weaknesses can be mitigated.

The key factor is that although it may not be possible to completely prevent devices being stolen, processes and procedures should be in place to recognise, at the earliest opportunity, that a device has gone missing and for this event to be reported to the appropriate management, the local police, the Dedicated Cheque and Plastic Crime Unit (DCPCU) (see appendix A), the equipment vendor and card acquirer.

5.3.4 Asset management

PEDs and terminals are valuable assets and must be subject to good management routines. Owners of assets (retailers, acquirers etc.) should devise an inventory of equipment to record serial numbers of devices and their location whether they are installed, or are replacements or spares. Regular checks should be carried out to ensure that devices are where they should be and that any changes are authorised and noted in the asset management record.

Consideration should be given to extending the use of any asset tagging used on other valuable equipment, like computers, to cover PEDs and terminals and these should be tamper evident and preferably customised to the retailer brand.

5.3.4.1 Electronic polling of devices

An effective management method is to audit attached devices electronically and automatically using their unique electronic serial numbers and logging the serial number against location. Contact should be made with the device vendor to find out how the PED can be interrogated to supply this information. A register of devices owned and allowed to be connected to the system should be recorded and the devices actually connected to the system should be compared to this list by electronically 'polling' the point-of-sale. Any devices reported as lost or stolen should be flagged as such on the system, then any device found on the network that is not on this list or is flagged as suspect should be prevented from working and appropriate alerts be raised. In performing an electronic 'polling' audit the information recorded should not just be whether or not the device is allowed but preferably the device's location within the system should be recorded i.e. the till it is attached to and in which store.

Consideration should be given to flagging devices as suspect that were registered as working but did not appear in the last audit as being active.

An intelligent solution should be implemented such that only registered devices will work with the rest of the system or terminal. Where such a capability exists consideration must be given to the following:

- The frequency of device interrogation, i.e. how often should the systems audit themselves. A minimum of once a day is recommended and several times a day is preferred;
- What alerts should be issued when a device is no longer present or an alternative device detected (genuine or rogue);
- Who is responsible for reviewing audit logs – it is preferable if this is done by two people separately;
- The escalation procedures that should be in place when errors are detected.

In alerting staff, care must be taken to only advise trusted staff and within some organisations this may mean that no-one at store level is alerted but a central security team handles the whole process. This becomes a careful balance between central control and the risk of local collusion that will have to be determined by each retailer's operational security processes.

Where electronic audits are carried out daily or at greater intervals it is recommended that the serial number of the PED is included in the transaction log file as this will provide valuable forensic evidence of when a bogus device was infiltrated into the system.

When a device is identified as suspiciously returning to the system after a period of absence, its location prior to its 'disappearance' should be recorded i.e. where was it and at what date and time.

5.3.5 Maintenance stock

Although not recommended some retailers may choose to have replacement equipment at store level to facilitate replacing faulty devices more quickly. These devices are an easier target for theft attempts and should be tightly controlled and audited on the same basis as devices installed in the store. Additionally any devices that are removed for repair should be returned securely and immediately to the agreed point and not kept at store level: see section 5.3.1 – Securing devices in storage and transit.

5.3.6 Software and configuration management

Inevitably changes will be made to the software and configuration of the point-of-sale environment for both EPoS systems and PoS terminals in order to accommodate changes to the card-processing environment. It is important that software and configuration changes are managed effectively. Although EPoS system software may not currently be a prime target for criminals, as other avenues of obtaining data are closed off system software attacks will become more attractive.

Terminal software is generally managed remotely by the terminal provider but it is essential that only authorised changes can be made to the device. Where the device is a PED connected to an EPoS system the PED provider may supply software updates for the retailer to distribute to his points-of-sale. It is essential that both the retailer and PED are able to validate the source of the software or configuration changes.

5.3.7 Key management

Key management routines must be managed in accordance with the payment schemes rules and regulations and follow the advice set out in UK Cards – Card Acceptor to Acquirer Interface Standards – Standard 70.

5.3.8 Payment card industry standards

5.3.8.1 Data security (PCI-DSS)

The international payments schemes have defined a set of security standards for the protection of sensitive cardholder data; these are laid out in the Payment Card Industry Data Security Standard. In support of these requirements the schemes have specified a layered audit process that all merchants must comply with. Details of the audit requirements are available from your acquirer.

5.3.8.2 Payment applications (PA–DSS)

The international payments schemes have further defined a set of security standards for payment applications and the management and processing of sensitive cardholder data; these are laid out in the Payment Application Data Security Standard.

5.3.8.3 PCI DSS Wireless Guideline

The international payment schemes have provided suggestions for the secure deployment of wireless local area networks (WLAN's) in retail environments. Their guidelines can be downloaded from the PCI-SSC site at:

https://www.pcisecuritystandards.org/pdfs/pci_dss_wireless_guideline_info_sup.pdf

5.4 Re-introduction of compromised devices

It is extremely difficult to eliminate stolen devices that the criminals can compromise as these may come from, for example, retailers who have ceased to trade where the devices have not been recovered. The best efforts are, therefore, to quickly, if not immediately, identify bogus devices that are being infiltrated into the system.

5.4.1 Asset lists

Part of the installation and activation process of an attached device should be the comparison of the device being installed to the list of 'allowed' devices. If the device being installed is flagged as suspect or does not appear on the 'allowed list' then it must be barred from the system and suitable alerts raised. As the 'allowed list' is vital to excluding bogus devices, care should be taken as to who has access to this list and its maintenance.

5.4.2 Engineer control

A common mode of operation is to use a bogus engineer who arrives on site to replace a faulty device or to perform a software or hardware upgrade. Retailers need to have in place a robust method and procedure for checking an engineer's credentials (job sheet, ID badge etc.) with information held at store level (for example, help desk numbers or head office contacts) rather than with contact information supplied by the engineer. Engineers should only be allowed on site if their attendance has been previously booked by a verifiable person within the retailer or maintenance agency.

Consideration should be given to requiring the person installing the PED to input a one-time password to enable the device on the network.

Any attempts to access in-store equipment where the 'engineer's' credentials do not match or where the 'engineer' leaves and doesn't return, whilst his credentials are being checked, should be reported to the nominated member of local or head office staff responsible for security. It is recommended that retailers put in place security policies and that staff are trained in what these policies are and what they are required to do if any are breached.

5.5 Detection of compromised devices

If devices are infiltrated back into the live environment then early detection is crucial to limiting the impact of any resultant fraud.

5.5.1 Asset management

As described in Section 5.3.4 – Asset Management, the asset tracking process and procedures should identify devices at the point of re-introduction but, depending on when a system self-audit is performed, this may not be immediate.

5.5.2 Staff

Staff can be the most valuable resource in detecting rogue devices as those most familiar with devices are the first to notice when "something isn't right". Visible asset tagging that is checked each morning when signing onto the till or when delivering the float for the till can provide a simple means of identification.

5.5.3 Store electronic sweeping

Some devices used in compromised PEDs use wireless networking technology to communicate with the criminals who will be in a parked vehicle in the vicinity. Equipment is available to perform an electronic sweep of a store to detect the radio signals emitted by these devices. These devices may be obtained from electronics or hobby retailers, or retailers specialising in surveillance equipment.

However, care must be taken to avoid false positives caused by legitimate wireless-based equipment in the store.

5.5.4 Bug detectors

Other devices used in compromised PEDs use GPRS mobile phone technology to communicate with the criminals who can be anywhere in the world. Devices are available that can detect the device synchronising with the network. The effectiveness of this type of device is still under evaluation.

5.5.5 X-raying devices

Access to an X-ray machine – usually used by retailers for screening incoming mail – is a valuable tool for identifying devices that have been compromised. The equipment vendor should be able to supply an image of what an unaltered device looks like when scanned.

Case Study 3 – What to Look For

A simple visual check of the point-of-sale environment can be very valuable in identifying equipment that has been tampered with or where something isn't right. There are a number of obvious things to look for when checking:

- Does the point-of-sale device look the same as the one that was there before? As with most equipment, devices will develop their own unique physical characteristics under normal wear and tear, and will collect scratches and marks that you will be familiar with. A quick look round may alert you to something suspicious.
- Is there evidence of the device being tampered with? Look for extra wires or physical damage to the casing, check the card entry area of the card reader to see if anything been inserted into it? Skimming devices are very difficult to spot but the evidence will be there.
- A quick scan around the till point might help spot anything unusual like a bugging device inserted into the phone lines.
- Check to see if the ceiling tiles above the till point have been moved or whether there are signs that a camera has been inserted overhead.

Specialist Retail Environments

Clearly not all retailers operate the same way and many environments throw up unique security challenges. In our discussions with retail trade bodies we have identified two that are worthy of note in that they share common issues relevant to a number of retail sectors.

Portable / Mobile Terminals

Increasingly, merchants are turning to the use of mobile or portable card acceptance devices as a more flexible way of serving customers. Devices are now common in the transport networks and in the hospitality industry. Depending on how they operate, these devices have to pass additional security evaluations before they are deployed, in particular to protect any data transfer across the airways.

Because of the nature of the devices the real issue is that they are far more difficult to manage from an asset control perspective. Additional effort has to be put into controlling their usage and physical location.

To control usage it may be possible to password protect some of the devices so that they will only operate if a password has been successfully entered. If the password is only issued to trusted staff it is possible to exercise an element of control over its use.

Tracking its physical location is more difficult but, at the very least, you should ensure that devices are booked out to a specific individual or individuals and returned to a secure location at the close of business. Whoever is supervising the use of these devices should ensure that their physical condition is checked regularly to ensure that they have not been tampered with.

In the longer term it may be possible for manufacturers to build tracking devices into these devices but where possible and practical a good short-term solution might be to attach a stock control tag to the device so, if it is removed from a store, an alarm will be set off.

Unattended Devices

Perhaps one of the most vulnerable point-of-sale environment is one that is left unattended. Card payment acceptance devices are now found in all manner of locations from street parking machines to specialist vending machines seen at train stations and airports. The remote location of these devices make them vulnerable to attack and it is important that when machines are being serviced or replenished they are inspected to see if there is any evidence that they have been tampered with. Similar to cash machines they may have had false readers and keypads attached and a residue of glue may be an obvious sign that this has happened. It is just as important to report any incident of this nature as it is to report the loss or theft of a PED.

5.6 Operation environment

- Use CCTV to sweep the point-of-sale area. Cameras must be fixed such that the customer's PIN cannot be identified in the field of view. It should not be possible to re-direct them to observe PIN entry. Access to CCTV should be restricted to authorised staff and protected to ensure that it is not possible to interfere with the recordings[2];
- Routines should be implemented to check the physical state of the device on a regular basis to ensure that the device has not been tampered with. This may include 'sweeping' the store to detect devices broadcasting captured data or images via mobile telephone or WiFi technology. Checks should include an inspection of the legitimate components of the card acceptance device and also the cabling to ensure that nothing has been added into the circuit.

2. See also Information Commissioner's CCTV Code of Practice www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

5.7 Activity matrix

The activity matrix shown in Table 1, below, shows the phases of the Theft, Re-introduction and Detection cycle that achieve the best results.

Table 1 Activity Matrix

Activity	Theft	Re-introduction	Detection
Physical Restraint	✓	✓	✓
Staff Training	✓	✓	
Asset Management		✓	✓
Electronic Polling	✓†	✓	✓
Asset Tagging		✓	✓
Weighing & Balance			✓‡
X-ray Machine			✓

† Electronic polling cannot prevent theft but can assist in detection.

‡ Weighing devices is not foolproof but may identify devices that need further investigation. Also the balance of the device (where its centre of gravity is) may also indicate a compromised device.

6 Reporting and evidence

It is important that information concerning the theft of PEDs and the suspected compromise of PEDs is correctly reported and recorded. Thefts need to be reported to your local police in order to obtain a crime report number (this will be needed for any insurance claim) and for intelligence gathering (see Appendix C, C.1.1 PED theft).

In the event that a suspected compromised device is identified then the procedure outlined in Appendix C, C.1.2 PED compromise should be followed. It is important that as much evidence as possible is gathered and protected to enable the police to pursue and prosecute those involved.

In both cases, but particularly where a compromised device is identified, the management of the process for retrieving the compromised device, securing any CCTV data and liaising with the police must be by a trusted member of staff or senior management. The local staff in the store should be excluded as far as possible in case collusion has been a factor in the placing of a compromised device.

6.1 Roles

Larger retailers have dedicated security staff, often ex-police officers, who manage all aspects of fraud within the company from shoplifting to IT security. These retailers are able to create a team of trusted employees who can audit and oversee the tasks of securing the point-of-sale environment. Specifically they can be brought into action when a compromised device is identified, in case a member of staff at the compromised outlet is colluding with the criminals either willingly or unwillingly.

Smaller retailers do not have the same level of resource available but senior managers and directors of these companies must take on these roles. The key is creating a number of trusted members of staff who can be relied on to manage any suspected security breaches and co-ordinate efforts to identify the perpetrators.

6.2 Useful things to do

One of the most important elements of any subsequent investigation will be to determine the length of time any compromised device may have been in service. This will help identify those card accounts that have been put at risk. If possible retailers should log and record the period of time when a device has been in service.

If CCTV is unavailable note which members of staff are working at the time, they may have valuable information that could help subsequent enquires.

7 Disposal

Asset management does not end until the asset has been destroyed in an authorised manner. This includes compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive.

The Waste Electrical and Electronic Equipment (WEEE) Directive came into force in January 2007 and aims to both reduce the amount of WEEE being produced and encourage everyone to reuse, recycle and recover it. The WEEE Directive also aims to improve the environmental performance of businesses that manufacture, supply, use, recycle and recover electrical and electronic equipment.

To this end, when devices have come to the end of their useful life through damage or are beyond repair, they must be disposed of in a manner compliant with the WEEE Directive. This disposal should be contracted to a company licensed to undertake this work and part of the specification of requirements to the contractor should be the destruction (usually by pulverisation) of unsalvageable components. PED enclosures, although made of low value plastic, are of high value to the fraudster to create bogus devices and these should be pulverised. The contractor should be required to supply a certificate of destruction on completion of the work.

8 Quick wins

8.1 Electronic asset management tags

Many retailers employ electronic tagging of items within store because of their high value or because of purchase restrictions, for example knives and alcohol. It is a simple process to extend this tagging to assets used in the payment process. This may not prevent devices from being stolen but it makes stealing the asset more difficult.

8.2 Unique asset management tags

As well as using in-store electronic asset tagging, the use of physical asset tags should be considered and the use of high quality tags incorporating a hologram are preferred. A hologram does not necessarily improve the asset control but may tend to raise staff perceived value of the device.

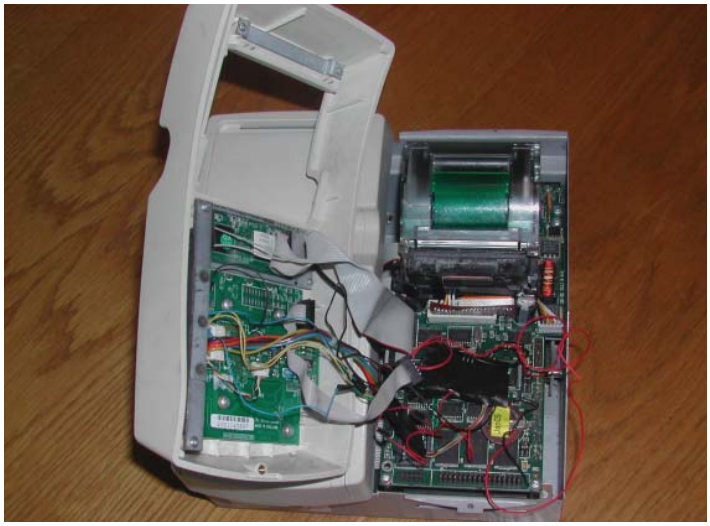
8.3 Weighing devices

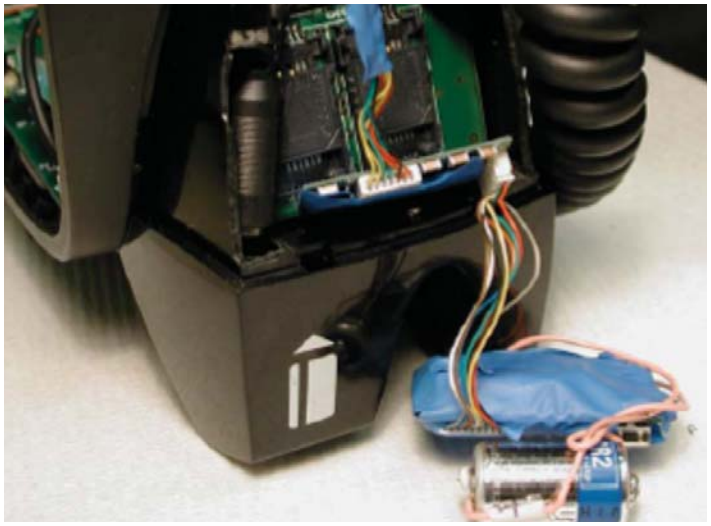
As PEDs and terminals are made to quite exacting standards and devices of the same build type will have the same component count they will, therefore, weigh the same within a good tolerance. Some vendors are already supplying the sample weight of their devices. If a criminal has added a 'bugging' device to a compromised device then it must weigh more than an 'original' device and simply weighing devices, at the point-of-sale, particularly where the checkout has built-in scales is a quick and simple way of identifying suspect devices.

This is not a foolproof method as the weight of devices may vary by production run, the type of cabling attached may vary and the criminals may have reduced the thickness of the device case to compensate for the introduced components.

8.4 Examples of compromised devices

To give you an idea of the types of attack criminals use to skim cardholder data, the following images show examples of real devices used by fraudsters in the UK.





Appendix A

A.1. Sources of information

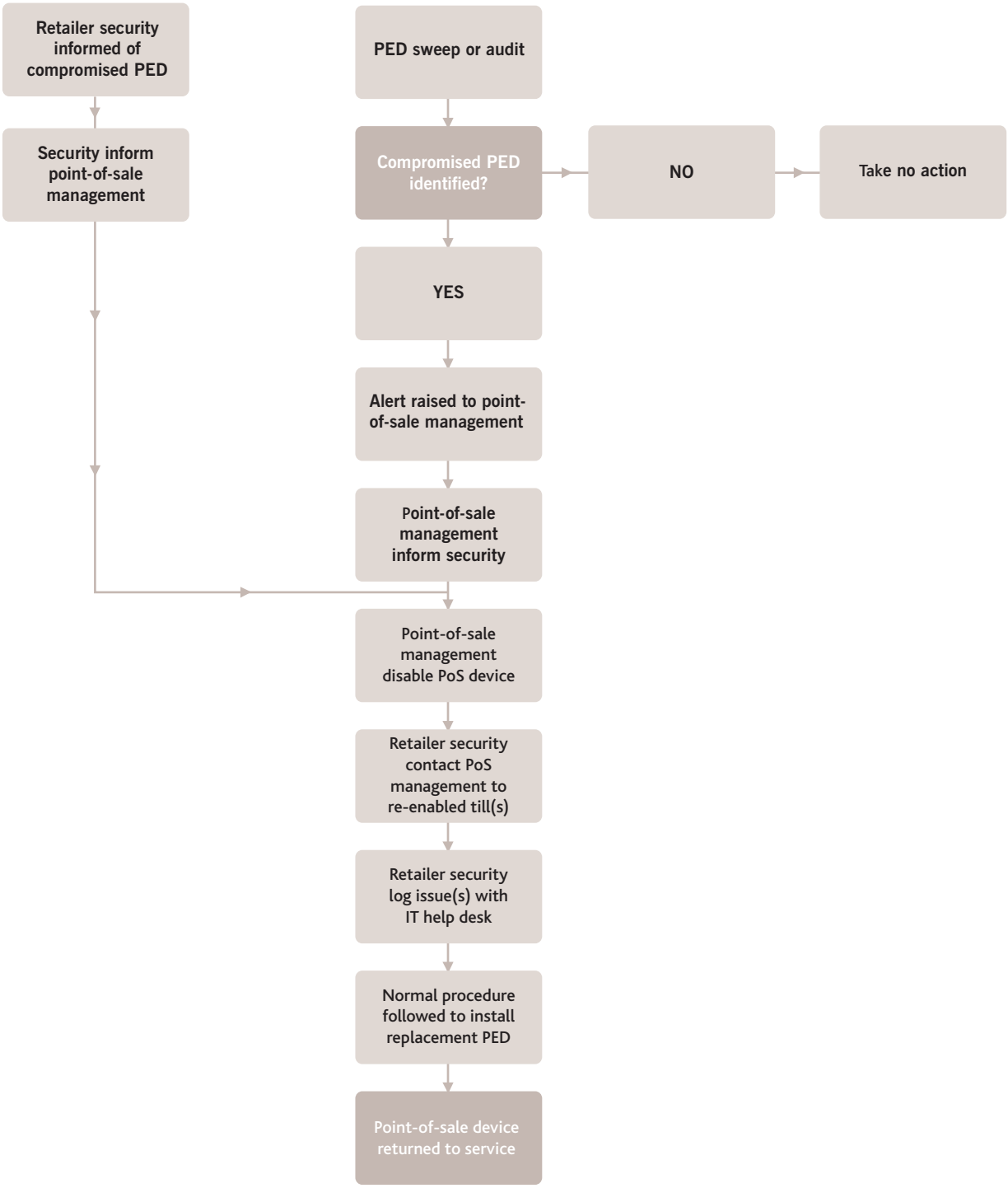
Additional advice and guidance is available from the international payment schemes and this can be obtained from the following sources.

Common Criteria	**http://www.commoncriteriaportal.org/**
Crimestoppers	**http://www.crimestoppers-uk.org/**
EMV Co	**http://www.emvco.com**
Information Commissioner's CCTV Code of Practice	**http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf**
MasterCard	**http://www.mastercard.com/us/sdp/index.html**
PCI Security Standards Council	**https://www.pcisecuritystandards.org**
The UK Cards Association	**UK Cards – Card Acceptor to Acquirer Interface Standards – Standard 70 APACS PED Protection Profile Version 1.37 Both available from http://www.theukcardsassociation.org.uk**
Visa EU	**http://www.visaeurope.com/aboutvisa/security/ais/main.jsp (in particular see downloads & resources) https://partnernetwork.visa.com/vpn/global/category.do?userRegion=1&categoryId=61&documentId=94**
Environment Agency WEEE	**Waste Electrical and Electronic Equipment http://www.environment-agency.gov.uk/business/regulation/31975.aspx**

Appendix B

B.1 PED Compromise notification

Figure 3. PED Replacement Process Flow



Appendix C

C.1. Action for stolen or compromised devices

As well as following the process described below the retailer should report any thefts to their acquirers.

The Dedicated Cheque and Plastic Crime Unit (DCPCU) can also be contacted on:

020 7382 2960

email – dcpcu@dcpcu.pnn.police.uk

C.1.1. PED theft

If you discover that a PED has been stolen:

1) Complete the pro-forma form Stolen PED notification, available to download from www.cardwatch.org.uk
2) Contact your local police and report the theft (obtain a crime report number);
3) Secure any CCTV images of the theft;
4) Retain any other evidence such as details of witnesses, staff or otherwise for the investigating officer;
5) Advise the DCPCU on the above telephone number or by email and they will liaise with the local police;
6) Follow any other procedures in line with your own company's policy.

C.1.2. PED compromise

If you believe that one or more of your PEDs have been compromised or tampered with:

1) Remove the device and retain securely. Seal in a tamper-proof bag if available;
2) Record the exact date and time the PED was disconnected from the system or 'powered down';
3) Report the incident to your local police;
4) Complete the pro-forma form PED compromise notification (available to download from www.cardwatch.org.uk) and advise the DCPCU of the incident. They will liaise with your local police to make arrangements for the collection of the device or otherwise;
5) Contact your company security and comply with any other company policy;
6) Secure any CCTV evidence and retain staff records.

THE
UKCARDS
ASSOCIATION

Mercury House, Triton Court,
14 Finsbury Square, London EC2A 1LQ
Tel: 020 7711 6200
www.theukcardsassociation.org.uk

In partnership with

Financial Fraud Action UK
Working together to prevent fraud

Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud prevention, presenting a united front against financial fraud and its effects. It was launched on 6 July to replace the work carried out by APACS and is now the payments industry voice on fraud. Financial Fraud Action UK (www.financialfraudaction.org.uk) works in partnership with The UK Cards Association on industry initiatives to prevent fraud on credit and debit cards.