Video Surveillance Systems
Chip and PIN guide

September 2018

For other information please contact:
British Security Industry Association
t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk

1. Introduction

This document offers guidelines to retailers and installers as to how a Video Surveillance System (VSS) should be used in conjunction with chip and PIN terminals.

The 14th February 2006 saw the full implementation of the chip and PIN programme. This primarily means that card issuers can only guarantee payment by chip and PIN card when the PIN is used, and may decline transactions when a signature alone is used (PIN bypass transaction). Consequently, signature only transactions become the retailer's sole liability. However, the exception to this rule is in the situations where chip and signature is used and is recognised by card issuers which include:

- people with a disability, who have registered as such with their bank, and
- overseas card holders.

In the case of contactless payments, for added protection from fraud, occasionally cardholders will be asked to insert the card and enter their PIN number, therefore this guide also applies to readers predominantly designed for contactless payments, as occasionally cardholder's will be entering their PIN numbers.

Increasing numbers of VSS systems are being used effectively in stores and at the point of sale to reduce loss of stock. Consideration should be given to how VSS can be used to further benefit retailers using chip and PIN and prevent the misuse of cardholder data.

2. Positioning of terminals

Chip and PIN terminals should always be placed in a location that allows customers to use the terminal in a manner that obscures any other customers or retailers from viewing the PIN number being entered. Signage should be installed to encourage customers to always shield the terminal with one hand while entering their PIN with the other. The use of non-fixed and fully portable chip and PIN terminals should allow customers privacy while entering PIN numbers.

3. VSS at the point of sale

At specific customer pay areas, the following guidelines should be applied to ensure that cardholders' confidential PIN data is not viewed and recorded when entered at the terminal.

a. Fixed cameras should be positioned so that in their field of view, the customers' personal PIN information cannot be clearly identified (i.e. looking face on towards the customer and not from behind and overhead).

b. Where cameras installed for the purpose of transaction monitoring unavoidably overlook PIN terminals, cardholders' data should be protected, either by physical or electronic means.

c. Moveable cameras (fully functional domes etc.) should be positioned, so that at no time during their operation, or in a preset position, can they clearly view the customers PIN information at the time of the transaction. Preset fields of view should be documented so that they can be clearly identified, and can be audited so that they cannot be subsequently altered or overridden by unauthorised persons.

d. Recording equipment should be kept in a secure environment and accessed only by authorised users.

e. Due to the growing use of mobile PIN terminals, it is essential that care be taken to ensure that they are only used in areas where surveillance cameras cannot clearly observe the cardholder's confidential PIN information.

f. Where the image requirement is to capture an identification image, this can often be best achieved by installing surveillance cameras at the exit doors viewing every person leaving the premises, instead of at the counter/till positions. A surveillance camera providing a view of the counter/general area will support the images captured at the exits.

4. Electronic point of sale (EPOS) recording systems

Some VSS systems are integrated with an EPOS system to record images and data associated with the transaction.

Care must be taken to ensure the live and recorded images exclude cardholders PIN data by applying the guidelines regarding the citing of surveillance cameras and shielding of PIN terminals in line with section 3 above.

5. Reference documents

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or updates) applies.

a. PCI Data Security Standard

The Payment Card Industry (PCI) Data Security Requirements apply to all those who store, process or transmit cardholder data. Additionally, these security requirements apply to all 'system components', which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include, but are not limited to: firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to: web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external (web) applications.

It is quite clear from the above that VSS components could be classed as 'system components' and moreover that Digital Video Recorders (DVRs) with Network capability and Network Video Recorders (NVR) can be classed as a 'network component, or server'.

b. Information Commissioner's Office 'In the picture: A data protection code of practice for surveillance cameras and personal information'

Particular attention should be paid to Section 6, selecting and siting surveillance systems.

c. Surveillance Camera Commissioners' - Surveillance Camera Code of Practice

This explains the guiding principles for the operators of VSS.

6. Other References

BS 7958 Management and Operation of CCTV
BS 7858 Security Screening of Personnel
General Date Protection Regulations (GDPR)
Data Protection Act 2018
Human Rights Act 1998
Freedom of Information Act 2000
BSIA CCTV Privacy Masking Guide
BS EN 62676-4 Video surveillance systems for use in security applications. Application guidelines
BS 8418 Code of practice for installation and remote monitoring of detector activated CCTV systems
BSIA Form 172 - Basic Guide for Installers to BS 8418 Systems
BSIA Form 196 – BS 8418 User Guide to a Detector Activated Remotely Monitored CCTV System
ISO 27001Information Security Management – Specification with guidance for use
BIP 0008 Code of practice for legal admissibility and evidential weight of information stored electronically

7. Document history

Date	Issue	Comment
30/10/06	Issue 1	First issue
28/01/12	Issue 1.1	Reconfirmation of 5yr review.
11/09/18	Issue 2	5 year review – minor updates

This document was created by the Video Surveillance Systems (CCTV) Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

Video Surveillance Systems (VSS) have had a profound impact on crime prevention and detection. The UK leads the way in the application of VSS and its use is wide-ranging, encompassing facial-recognition technology, remote video monitoring, video smoke detection, mobile systems and Automatic Number Plate Recognition as well as many other functions.

In order to provide guidance and simplification in the complex area of VSS, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The VSS Section encourages debate on new developments and concerns, such as digital video evidence and facilitating communication protocols between different manufacturers' products. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, users, the police, inspectorates and insurers. The section also works with government on these issues.

VSS must be operated responsibly in order to respect citizens' rights and maintain public confidence. Laws such as the Data Protection Act have an important role to play in achieving this. BSIA VSS companies drive best practice in this area and can provide advice on how VSS users can adhere to the relevant legislation.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Anbrian House
1 The Tything
Worcester
WR1 1HD

t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk