Use of the Police National Computer by non-police organisations

An inspection of Post Office Limited

May 2016

© HMIC 2016

ISBN: 978-1-78655-089-7

www.justiceinspectorates.gov.uk/hmic

Contents

Introduction

Background and context

The Police National Computer (PNC) is a national database of information available to all police forces throughout the United Kingdom.[1] In addition, certain other organisations, referred to as “non-police organisations”, have access to information held on the PNC in order to help them fulfil their statutory functions.

In such instances, access is granted by a body called the Police Information Access Panel ("the Panel").[2] In order to obtain access, each organisation must submit a detailed business case that satisfies the Panel that a valid and lawful requirement for access exists.

If this is the case, two documents are produced that specify the level of access permitted and the manner in which the non-police body may use the PNC: the *Supply Agreement*, which describes the permitted access and how it will be provided, and the *Security Operating Procedures*, which are a requirement of the *Supply Agreement* but which are produced by the non-police organisation for the attention of its staff.

Some non-police organisations access the PNC through discrete computer terminals installed in their premises. This is known as “direct access”. Other non-police organisations obtain PNC information through a third party, usually a police force. This is known as “indirect access”.

In either arrangement, the public needs to have confidence that access is properly regulated and that effective auditing arrangements are in place. This is important because much of the information held on the PNC is sensitive and personal.

Her Majesty's Inspectorate of Constabulary (HMIC) is recognised as having strong expertise in this area and the Government’s Independent Advisor on Criminality Information Management recommended that HMIC’s audit role is extended to cover all PNC users.[3]

---

[1] *Police National Computer (PNC) Guidance: version 5*, Home Office, January 2014, page 5. The PNC holds information concerning people and property, including convictions, wanted and missing people, stolen vehicles and other types of stolen property.

[2] The Police Information Access Panel is a sub-group of the PNC governing body – the Police PNC Policy and Prioritisation Group (known within policing as "P4G"). The Panel is chaired by a chief officer and comprises a cross-section of senior Home Office and police leaders who are concerned with the management of the PNC. The Panel meets on a quarterly basis to consider applications for access to the PNC. Her Majesty's Inspectorate of Constabulary is represented on the Panel.

[3] *A Common Sense Approach: a review of the criminal records regime in England and Wales*, Sunita Mason (Independent Advisor for Criminality Information Management), November 2011, pages 34-35.

Consequently, as part of our regular programme of inspections,[4] we examine: the circumstances under which non-police organisations are granted access to the PNC; the ways in which they use PNC information; the safeguards that are required in order to protect the information; and whether those safeguards are being properly applied.

Non-police organisations are also subject to a separate Home Office audit, which examines in detail whether PNC data is held and used in an approved and secure way.[5]

While HMIC's inspections can be prioritised on the basis of the findings of these Home Office audits, HMIC's inspections do not examine all of the same issues. However, there can be certain areas of overlap. Where our inspections reveal concerns in areas that are also subject to Home Office audit, we highlight this.

Terms of reference

HMIC's inspections of non-police organisations that have access to the PNC aim to answer three questions:

1. Is the level of access specified in the *Supply Agreement* appropriate for the needs of the non-police organisation?

2. Does the non-police organisation comply with the *Security Operating Procedures*? In particular, are the arrangements for training, physical security, and internal audit compliant with the *Security Operating Procedures*?

3. Is the non-police organisation making efficient and effective use of the PNC?

About Post Office Ltd

Post Office Ltd, which we also refer to in this report as "the Post Office" and "the organisation", has direct access to the PNC.

This state-owned organisation came into existence in April 2012 when the Royal Mail and Parcel Force were privatised. Through post office counters, it provides a wide range of financial products and services including banking, insurance and mortgage lending. Post Office Ltd also runs cash depots and manages a fleet of approximately

[4] *HMIC's 2015/16 Inspection Programme: An inspection framework prepared under Schedule 4A to the Police Act 1996*, HMIC, March 2015. Available from: www.justiceinspectorates.gov.uk/hmic/publications/hmic-inspection-programme-2015-16/

[5] The Home Office National Police Information Risk Management Team conducts audits to assure the Police Information Access Panel that PNC data is being held and used in an approved and secure manner in accordance with the supply agreement and relevant legislation, including but not limited to the Data Protection Act 1998, the Computer Misuse Act 1990 and the Official Secrets Act 1989.

400 cash-in-transit vehicles serving post offices and other businesses. These aspects of the Post Office's operations are risky because they involve the custody and movement of large quantities of cash.

Methodology

This inspection took place in November and December 2014. Before the fieldwork stage, we reviewed documents (including the *Supply Agreement* and the *Security Operating Procedures*) to assist us in preparing questions for the interviews.

We invited Post Office Ltd to provide us with documentary evidence of its adherence to the *Supply Agreement* and *Security Operating Procedures*. This was followed by a visit to Post Office Ltd's control centre in Bradford (at which the organisation's single PNC terminal is housed). Over two days, we assessed the physical security arrangements and interviewed Post Office staff who use the PNC, including the manager, supervisors and PNC operators. We asked interviewees to show us how they used the PNC.

We examined the Post Office's internal audit process for the PNC. We looked at audit records and, through our interviews, tested interviewees' understanding of the internal audit processes and escalation procedures.[6]

We also reviewed data relating to Post Office Ltd's use of the PNC. These data were provided to us by the Home Office.

[6] In this context, escalation procedures are the procedures that personnel are expected to adopt when an internal audit reveals that a PNC check has been conducted for an inappropriate purpose. Generally, the procedure involves referring the matter to a manager.

Findings

Scale of PNC use

The Home Office provided us with statistics on the number of PNC checks carried out by Post Office Ltd for the period 1 January 2014 to 31 December 2014. We found that 52 PNC checks in relation to people were carried out by Post Office Ltd over that period. There were additionally 31 vehicle checks as well as 21 transactions that enabled the manager to check that use of the PNC had been legitimate.

The level of access and authorised purposes for PNC use

We found that the Post Office was using the PNC in accordance with the decisions of the Police Information Access Panel, although those decisions had not been accurately transcribed into the *Supply Agreement* and *Security Operating Procedures*.

The level of access available to Post Office Ltd was sufficient to enable basic checks against people and more comprehensive checks for vehicles. We compared the Post Office's use of the PNC against the level of access that had been authorised and found that it had not been making use of the full range of checks that had been made available.

Level of access

We were provided with a copy of the current *Supply Agreement*, which was agreed between Post Office Ltd and the National Policing Improvement Agency on 18 May 2012 and was to continue in force for three years. The National Policing Improvement Agency was abolished in 2013 and as a result, responsibility for the PNC was transferred to the Home Office. Paragraph 6 of Schedule 8 to the Crime and Courts Act 2013 provides for the *Supply Agreement* to continue to have effect once responsibility for the PNC had been transferred to the Home Office, without the need for adoption of a new *Supply Agreement*.

The *Supply Agreement* specifies that Post Office Ltd was authorised to conduct five different kinds of PNC check:[7]

1. Name (restricted): this type of check allowed an operator to type in the name of a person in order to determine whether the PNC holds a record of someone with that name. If such a record existed, the Post Office Ltd level of access allowed it to view certain information from that record, such as criminal

[7] *Supply Agreement Version 1.0,* National Policing Improvement Agency and Post Office Ltd, May 2012, Part 2 Schedule 1, paragraph 1.3.

convictions, arrest details and cautions. For this kind of check, Post Office Ltd's access was restricted to particular parts of the record.

2. Vehicle registration mark (basic): this type of check allowed an operator to type in a complete vehicle registration mark in order to determine if the vehicle was stolen or of interest to the police for some other reason. This type of check also revealed the name and address of the vehicle's registered keeper.

3. Vehicle registration mark (part): this type of check allowed an operator to type in a part of a vehicle registration mark in order to identify all vehicles with a registration mark that included the part of the registration mark that was used to make the search.

4. Postcode: this type of check allowed an operator to type in a postcode (or a combination of postcodes up to a maximum of six) in order to identify vehicles registered to an address within the area covered by the postcode that was used to make the search.

5. Transaction log: this type of check allowed an operator to type in a code in order to generate a list of previous checks carried out on the PNC. Generally this list was used for audit purposes.

In addition, in 2012 the Police Information Access Panel had approved an application from Post Office Ltd for access to three additional types of PNC check, which permitted searching for vehicles based on their description rather than their registration mark. Technical access to these checks had subsequently been made available by the National Policing Improvement Agency, although the *Supply Agreement* had not been updated to reflect this.

We found, however, that the Post Office was not making full use of the access that had been authorised. We found that no postcode or partial vehicle registration mark checks had been conducted in 2014, and no use at all had been made of the enhanced vehicle checks that allow searching on factors other than the vehicle registration mark, since access had been granted in 2012.

Authorised purposes

The *Supply Agreement* stated that Post Office Ltd was authorised to conduct PNC checks for the following purposes:[8]

- "Assisting [Post Office Ltd] investigators with the investigation of specific criminal offences within their remit and in accordance with the Statutory Codes of Practice.

[8] *Ibid.*, Part 2 Schedule 1, section 2.

- Obtaining the previous convictions of alleged offenders and witnesses who have provided written statements, in cases being prosecuted or under active consideration for possible prosecution by [Post Office Ltd].
- In order to carry out risk assessments for health and safety purposes on the identified occupants of premises/places of residence which are to be searched/or subject of an operation by [Post Office Ltd] investigators."

Our interviews did not reveal any areas of concern in relation to Post Office Ltd's access to the PNC.

Does the organisation comply with its Security Operating Procedures?

We found that Post Office Ltd was compliant with the requirements set out in its *Security Operating Procedures*. However, some PNC requests were submitted on handwritten forms, and where there was no corresponding record on the incident management system, this meant the audit trail was not as robust as it should have been.

We also found that the *Security Operating Procedures* described the purposes for which PNC use had been authorised in a way that did not match the purposes described in the *Supply Agreement*. This was because the *Supply Agreement* had not been updated when the Panel had authorised the Post Office's use of additional types of vehicle check. This made it difficult for Post Office staff to be certain about the purposes for which PNC access had been authorised.

Training

One of the requirements of the *Security Operating Procedures* is that all PNC users must receive accredited training.[9] While at the control centre we asked Post Office Ltd to show us the relevant training records. These were extensive and satisfied us that all the Post Office's PNC users had received accredited training.[10]

Physical security

A further requirement of the *Security Operating Procedures* is that the PNC terminal must be located in a secure building.[11]

We found that the Post Office's PNC terminal was kept in a secure building – and thus complied with the requirement – but the level of security was excessive.

[9] *Security Operating Procedures Version 1.5*, Post Office Ltd, September 2014, paragrapgh 4.1.

[10] The College of Policing is responsible for the accreditation of PNC training providers.

[11] *Security Operating Procedures Version 1.5*, Post Office Ltd, September 2014, paragraph 3.8.

The PNC terminal was located in an unoccupied office within the Post Office control centre. Once inside this office we found that the PNC terminal was encased in a locked cabinet, the keys for which were kept in the control centre. This, and the PNC's electronic security (unique user names and passwords), made conducting a PNC check a lengthy process; in all, there were six layers of physical security surrounding the PNC terminal. This exceeds the security arrangements in place for the PNC terminals in most police forces.

We also found that the normal practice at the control centre was for the PNC terminal to be turned off when not in use. This extended the length of time it took from receipt of a request for a PNC check to completion of the check. A PNC-trained member of staff showed us that it took approximately ten minutes from a request being made to the result being provided. This was excessive, as a PNC check under normal circumstances should take less than twenty seconds.

From interviews with control centre personnel we determined that the low number of checks and lack of use of certain kinds of check were due to a combination of the delay caused by the security arrangements and a lack of awareness within the organisation of the business benefits of the PNC.

Internal audit

The *Security Operating Procedures* and other related documents set out various requirements that are the subject of internal audit. These include:

- PNC personnel are required to sign a document to confirm they have read the *Security Operating Procedures* and undertake to comply with them;[12]
- PNC checks may only be conducted once authorised by an authorising manager at least one grade senior to the requesting officer (in urgent cases, orally, otherwise in writing);[13] and
- the frequency of audits will depend on the amount of transactions but for less regular use, a weekly audit with reporting monthly will be appropriate.[14]

In relation to the first requirement, we examined the documentation and were satisfied that all PNC users had signed the appropriate document.

In relation to the second requirement, we found that requests for PNC checks were sometimes made via radio by cash-in-transit vehicle drivers who were concerned for their security. Radio requests for PNC checks were recorded on the Post Office computerised incident management system. We found that, in instances where a

[12] *Ibid.*, paragraph 9.7.6.

[13] *Ibid*, paragraphs 4.2 and 9.8.1.

[14] *Ibid*, paragraph 9.4.

request over the radio was urgent and an authorising manager was not immediately available, the requests were being reviewed and authorised retrospectively. We consider this to be good practice.

PNC requests in other cases were submitted either via email as electronic documents or by hand-written completion of the electronic document template. In both cases, the completed forms were kept as hard copies in a file.

The audit records we examined indicated that, whether the request originated with a radio call from a cash-in-transit driver or completion of a request form by an investigator, the requirement for authorisation of each PNC check was being met.

In relation to the third requirement, we found that Post Office Ltd was auditing all of its PNC checks immediately after they were carried out. Because of the low numbers of checks, this was not an onerous task for the organisation.

Our examination of the internal audit arrangements revealed that the submission of a hand-written request for a PNC check was not recorded on the Post Office's computerised incident management system. In such cases, although PNC records showed the date and time of access to PNC data, it was not always clear to us exactly when the request had been made and authorised. Consequently, integrity in the submission and authorisation process was less easy to assure.

We found clearly defined procedures for the escalation of issues of concern to managers. Although we did not find any instances where concerns had been escalated, those whom we interviewed were aware of and understood the procedures.

Conclusions

Level of access

Taking into account the purposes for which Post Office Ltd needs PNC access, we conclude that the level of access specified in the *Supply Agreement* for checks on persons is appropriate for the organisation's needs. However, given the lack of use of postcode and vehicle descriptive searching (in any event, the latter not being included within the *Supply Agreement*),[15] we recommend that the Police Information Access Panel reconsiders the necessity for such access.

Compliance

The comprehensive training records, the physical security arrangements, the signed undertakings by all PNC staff and the high level of internal audit coverage lead us to conclude that Post Office Ltd is complying with the requirements of its *Security Operating Procedures*. We recommend, however, that Post Office Ltd updates its *Security Operating Procedures* to ensure the same terms are used to describe the purposes for which PNC access has been authorised as are contained within the *Supply Agreement*.

We also advise Post Office Ltd to replace handwritten PNC check requests with submission of electronic documents by email in order to provide greater assurance of integrity in the process for obtaining information from the PNC.

Efficiency and effectiveness

With overly cumbersome security leading to delays in accessing the PNC, an average of fewer than one name or vehicle check each day and evidence that not all the available PNC facilities were being used, we conclude that Post Office Ltd could make more efficient and effective use of the PNC.

We advise Post Office Ltd to:

- make the PNC terminal more accessible to operators; and
- consider use of the Home Office's PNC presentations, posters and leaflets to improve staff awareness.

[15] Following this and other PNC inspections, HMIC understands that the Home Office replaced Supply Agreements with documents entitled *Agreement for the Supply of PNC data via Direct Access* and *Memorandum of Understanding Regarding the Supply of PNC data via Direct Access*. HMIC was informed that one of the former documents was issued to Post Office Ltd on 11 February 2016.

If these actions led to an increase in the number of PNC checks conducted, Post Office Ltd would have the option of reducing the frequency of audit to a level that would be more manageable and yet still proportionate.