Use of the Police National Computer by non-police organisations

An inspection of the Financial Conduct Authority

May 2016

ISBN: 978-1-78655-096-5

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 which 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 the 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 the 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 the Financial Conduct Authority

The Financial Conduct Authority, which we sometimes refer to in this report as the "the Authority", has direct access to the PNC.

Following the financial crisis of 2008, the Financial Services Act 2012 created a new system for regulating financial services to protect and improve the United Kingdom's economy. As a result, the Financial Conduct Authority was created, replacing the Financial Services Authority.

---

[4] *HMIC's 2015/16 Inspection Programme: An inspection framework prepared under Schedule 4A to the Police Act 1996*, HMIC, March 2015, page 11. 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.

The Financial Conduct Authority regulates the conduct of more than 70,000 businesses. Its aims are to ensure that the financial industry is run with integrity and that firms provide consumers with appropriate products and services. The Authority investigates complaints from consumers relating to the provision of financial services where that provision is alleged to have fallen below an acceptable standard. The Authority takes action against those who break financial rules by using its full range of criminal, civil and regulatory powers.[6] The Authority investigates and prosecutes various offences in relation to the financial services industry, such as insider dealing, market manipulation and terrorist financing.

Methodology

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

We invited the Financial Conduct Authority to provide us with documentary evidence of its adherence to the *Supply Agreement* and *Security Operating Procedures*. This was followed by a visit to the Authority's control centre in London (at which the Authority's three PNC terminals were housed). Over one day, we observed the physical security arrangements and interviewed Financial Conduct Authority staff who used the PNC, including the manager, supervisors and the PNC operators. We asked interviewees to show us how they used the PNC.

We examined the Financial Conduct Authority'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.[7]

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

[6] *Financial Conduct Authority Business Plan 2015/16*, Financial Conduct Authority, 2015, page 65.

[7] 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 the Financial Conduct Authority for the period 1 April 2014 to 30 September 2014. We found that 1,168 PNC checks in relation to people were carried out by the Authority over that period. There were additionally 101 vehicle checks as well as 96 transactions that enabled the manager to check that use of the PNC had been legitimate. There had been no use of the postcode check.

The level of access and authorised purposes for PNC use

We found that the Financial Conduct Authority had access to and was using the PNC even though the *Supply Agreement* had expired in May 2014.

Notwithstanding the lack of a current *Supply Agreement*, we found that the level of access available to the Financial Conduct Authority was sufficient to enable basic checks against people, vehicles and postcodes. We compared the Authority'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 postcode check at the time of our inspection.[8]

Level of access

We learned that, before the Financial Conduct Authority was formed, the Financial Services Authority obtained PNC access through a *Supply Agreement* with the National Policing Improvement Agency, dated 18 May 2011.[9] We obtained a copy of this signed agreement and found that it was valid for three years from 18 May 2011.

[8] Since our inspection took place we asked the Home Office to provide us with statistics on the number of postcode checks carried out by the Financial Conduct Authority for the period 1 January 2015 to 31 December 2015. We found that 23 postcode checks were carried out by the Authority over that period.

[9] 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 ("Continuity in relation to functions") provides for supply agreements to continue to have effect once responsibility for the PNC had been transferred to the Home Office, without the need for adoption of new *Supply Agreements*.

Since its formation in 2012, the Authority has made use of the PNC. However, we found that the *Supply Agreement* contained a clause that stated:

> "This Agreement is specific to the Customer who shall not assign, transfer, sublet or dispose of any rights, duties and obligations contained herein."[10]

Consequently, we sought to establish whether, notwithstanding this clause, the legal arrangements for the transfer of functions from the Financial Services Authority to the Financial Conduct Authority may have included provision for the transfer of PNC access from the Financial Services Authority to the Financial Conduct Authority. We were informed by the Financial Conduct Authority that the relevant legal arrangements did appear to include such a provision.[11]

We learned that the Home Office had not issued a new *Supply Agreement* when the 2011 *Supply Agreement* expired in May 2014. We found that the Financial Conduct Authority continued to have access to and make use of the PNC after that date and at the time of our inspection in 2014, despite the lack of a current *Supply Agreement*.

The expired 2011 *Supply Agreement* specified that the Financial Conduct Authority was authorised to conduct five different kinds of PNC check:[12]

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 Financial Conduct Authority's level of access allowed it to view certain information from that record, such as criminal convictions, arrest details and cautions. For this kind of check, the Financial Conduct Authority'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.

---

[10] *Supply Agreement Version 1.0,* National Policing Improvement Agency and Financial Services Authority, May 2011, Part 2, Schedule 4, paragraph 15.1.

[11] In its response to HMIC, the Financial Conduct Authority stated: "Section 1A(1) of the Financial Services and Markets Act 2000 provides that: The body corporate previously known as the Financial Services Authority is renamed as the Financial Conduct Authority". Based on its review of the relevant legislation, the Financial Conduct Authority considered that this provision would cover the use of the *Supply Agreement* as it signified a change in name only without change in legal status requiring renewal or alteration of legal agreements that were made with the Financial Services Authority prior to the formation of the Financial Conduct Authority.

[12] *Supply Agreement Version 1.0,* National Policing Improvement Agency and the Financial Conduct Authority, May 2011, Part 2, Schedule 1, paragraph 1.3.

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 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.

Authorised purposes

The *Supply Agreement* stated that the Financial Conduct Authority was authorised to conduct PNC checks for "the purpose of investigations and case preparations."[13]

This was vague and did not specify in enough detail what the Authority was allowed to use the PNC for. From our interviews with control centre personnel we determined that PNC checks were usually carried out on:

- people applying for certain roles in the financial services industry where there was reason to believe that they had a criminal record which they had not disclosed;

- people named in, or associated with, consumer credit applications including; first time applications or where permission for changes and variations in existing consumer credit controls are requested;

- people linked to investigations under the Consumer Credit Act 1974, whether individually or as part of what the Financial Conduct Authority called "high risk sector investigations", for example home lenders;

- people who were suspects or witnesses in Financial Conduct Authority criminal investigations and prosecutions; and

- people whom the Authority's investigation staff intended to visit in the course of an investigation. PNC checks in these cases were undertaken in order to inform health and safety risk assessments that were carried out prior to visits.

Our interviews did not reveal any areas of concern in relation to the Financial Conduct Authority's level of access to the PNC. Assuming that the Authority will

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

continue to have access to the PNC, we consider that the Police Information Access Panel should detail more specifically the purposes for which the Financial Conduct Authority may use the PNC.

Does the organisation comply with its Security Operating Procedures?

We found that the Financial Conduct Authority was compliant with the requirements set out in its *Security Operating Procedures*.

We also found that the *Security Operating Procedures* described the purposes for which the PNC use had been authorised in a way that did not match the purposes described in the *Supply Agreement*.[14] This was because the *Supply Agreement* had not been updated when the *Security Operating Procedures* were amended.

Training

One of the requirements in the *Security Operating Procedures* is that all PNC users must receive accredited training.[15] While at the control centre we asked the Financial Conduct Authority to show us the relevant training records. These were extensive and satisfied us that all the Authority's PNC users had received accredited training from an external training provider.[16]

Physical security

A further requirement of the *Security Operating Procedures* is that the PNC terminals must be located in a secure building.[17]

We found that the Financial Conduct Authority's PNC terminals were kept within a secure office located in a secure building. There were sufficient access controls in place. Furthermore there were identity pass checks at both the main gate and building reception. All visitors were met at reception and then escorted throughout the control centre by a member of Financial Conduct Authority staff. Once inside the control centre, the PNC terminals were located in a separate office that was locked when not in use. Only the PNC-trained staff had access to this office.

[14] *PNC Security Operating Procedures Version 1.9*, Financial Conduct Authority, November 2014, paragraph 2.1.

[15] *Ibid.,* paragraph 4.

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

[17] *PNC Security Operating Procedures Version 1.9*, Financial Conduct Authority, November 2014, paragraph 2.1.

Internal audit

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

- mandatory audits every month;[18]
- each transaction conducted on the PNC must be noted on a spreadsheet; and[19]
- if any transaction carried out by the users has not been approved or there are any other potential security breaches that may have occurred, the matter should be reported to the PNC Manager without delay.[20]

In relation to the first requirement we interviewed one of the trained independent auditors. We examined a sample of the audit reports and found the audits to be carried out regularly. The sample size of 10 percent of all checks was being audited satisfactorily. The PNC manager signed off all the audit results.

In relation to the second requirement we examined a spreadsheet that staff were required to complete, detailing every PNC check undertaken. This spreadsheet was completed correctly and was used in the audit process.

In relation to the third requirement 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.

We found that the PNC personnel were required to sign a document to confirm they had read the *Security Operating Procedures* and undertake to comply with them. We examined the documentation and were satisfied that all the PNC personnel had signed the appropriate document.[21]

[18] *Ibid.,* paragraph 12.2.

[19] *Ibid.,* paragraph 12.6.

[20] *Ibid.,* paragraph 12.8.

[21] *Ibid.,* paragraph 3.12 and Appendix A.

Conclusions

Level of access

We conclude that the Financial Conduct Authority needs direct access to the PNC and that the absence of a valid *Supply Agreement* is a serious matter that should be remedied at the earliest opportunity.[22]

We conclude that the level of access specified in the *Supply Agreement* is vague and recommend that the Police Information Access Panel defines more specifically the purposes for which the Authority has been given access to the PNC.

Compliance

The extensive training records, the satisfactory physical security arrangements, the signed undertakings by all PNC staff and the satisfactory level of internal audit coverage lead us to conclude that the Financial Conduct Authority has been complying with the requirements of its *Security Operating Procedures*.

Efficiency and effectiveness

We conclude that, but for the areas for improvement described above, the Financial Conduct Authority is making efficient and effective use of the PNC.

[22] Following this and other PNC inspections, we understand that the Home Office replaced *Supply Agreement*s 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*. We were informed that one of the latter documents was issued to the Financial Conduct Authority on 9 February 2016.