Scottish Information Commissioner
www.foi.scot

Decision Notice 256/2025

Rail Settlement Plan ticket specification and public keys

Applicant: The Applicant
Authority: Caledonian Sleeper Limited
Case Ref: 202500262

Summary

The Applicant asked the Authority for information relating to the Rail Settlement Plan ticket specification and public keys. The Authority withheld the information on the grounds that disclosure would, or would be likely to, prejudice substantially the prevention or detection of crime. The Commissioner investigated and found that the Authority had correctly withheld the information.

Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1), (2) and (6) (General entitlement); 2(1)(b) (Effect of exemptions); 35(1)(a) (Law enforcement); 47(1) and (2) (Application for decision by Commissioner).

Background

1. On 22 November 2024, the Applicant made a request for information to the Authority. They asked for

   - "Rail Settlement Plan Aztec ticket type '06' specifications - ordinary travel tickets
   - Rail Settlement Plan Aztec ticket type '08' specifications - digital railcards
   - Any other Rail Settlement Plan specifications you hold on the issuance of Aztec barcodes and/or digital tickets for the railways

- Public RSA keys/certificates used by you to issue such Aztec barcodes, in either X.509, PKCS#1, PKCS#12, or other appropriate format for conveying the public half of an encryption key.
- The same public keys of any other issuer who can issue digital tickets valid on rail services under your purview."

2. By way of background, Aztec ticketing refers to a barcoding standard commonly used for electronic tickets in railway systems. It is a type of 2D barcoding that can encode a large amount of data in a small space and is easily scannable.

3. The Authority responded on 20 December 2024. It explained that it did not did itself hold the information requested, but that it was held by the Rail Delivery Group (RDG) for train operators. It said that it accessed the information so that its ticketing suppliers could produce, read, encode or validate rail tickets. However, it stated that the information requested was exempt from disclosure under section 35(1)(a) of FOISA and explained why.

4. On 13 January 2025, the Applicant wrote to the Authority requesting a review of its decision. They disagreed that the exemption in section 35(1)(a) of FOISA applied and explained why.

5. The Authority notified the Applicant of the outcome of its review on 10 February 2025, which fully upheld its original decision.

6. On 17 February 2025, the Applicant wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA. They stated that they were dissatisfied with the outcome of the Authority's review because they disagreed that the exemption in section 35(1)(a) of FOISA applied.

Investigation

7. The Commissioner determined that the application complied with section 47(2) of FOISA and that he had the power to carry out an investigation.

8. On 13 March 2025, the Authority was notified in writing that the Applicant had made a valid application. The Authority was also asked to send the Commissioner the information withheld from the Applicant. The Authority provided the information, and the case was subsequently allocated to an investigating officer.

9. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. The Authority was invited to comment on this application and to answer specific questions related to its reasons for applying section 35(1)(a) of FOISA and its consideration of the public interest test.

Commissioner's analysis and findings

10. The Commissioner has considered all the submissions made to him by the Applicant and the Authority.

11. The Commissioner has endeavoured to give as full account of his reasoning as he can, but, as recognised by Court of Session in Scottish Ministers v Scottish Information Commissioner [2006] CSIH 8[1], at paragraph [18]:

"in giving reasons for his decision, [the Commissioner] is necessarily restrained by the need to avoid, deliberately or accidentally, disclosing information which ought not to be disclosed."

Section 35(1)(a) – Law enforcement

12. Section 35(1)(a) of FOISA provides that information is exempt information if its disclosure would, or would be likely to, prejudice substantially the prevention or detection of crime. This exemption is subject to the public interest test in section 2(1)(b) of FOISA.

13. As the Commissioner's guidance on this exemption[2] highlights, the term "prevention or detection of crime" is wide-ranging, encompassing any action taken to anticipate and prevent crime, or to establish the identity and secure prosecution of persons suspected of being responsible for crime. This could mean activities in relation to specific (anticipated) crime or wider strategies for crime reduction and detection.

14. The exemption in section 35(1)(a) of FOISA can only apply where disclosure of the information in question would, or would be likely to, prejudice substantially the prevention or detection of crime.

15. FOISA does not define “substantial prejudice”, but the Commissioner considers an authority would have to identify harm of real and demonstrable significance. The harm would also have to be at least likely and, therefore, more than a remote possibility. The authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice the exemption is designed to protect against.

16. The exemption is subject to the public interest test in section 2(1)(b) of FOISA.

The Applicant’s submissions

17. The Applicant disagreed with the Authority’s argument that disclosure of the ticketing standards and public keys (not private keys) would hinder the detection of fraudulent tickets. While they accepted that train ticket fraud was a major problem, they did not accept that disclosure of the information requested would hinder the detection of such fraud.

18. The Applicant submitted that enough information had been provided to them through responses to various FOI requests on this matter (and was otherwise publicly available) that they could confidently say that UK train tickets were protected with RSA cryptography.

19. The Applicant said that such cryptographic protections provided that without the private key (which they had not requested) “no party can forge tickets but the intended party”. They explained that train tickets were signed using these keys, ensuring a “mathematic binding” between the Authority and the tickets it issued – meaning it “would be trivial to detect attempted forgeries of tickets, as the signature verification would fail”.

20. The Applicant noted that such specifications for trains were either already provided openly by, or were obtainable on request from, the European Union Agency for Railways and other European train operators. They said that these specifications were provided with no

[1] https://www.bailii.org/scot/cases/ScotCS/2008/CSIH_08.html

[2] https://www.foi.scot/sites/default/files/2022-04/BriefingSection35LawEnforcement.pdf

detriment to the security of railway ticketing on the continent and that all of the ticket encodings implemented similar cryptography to that in UK train tickets. They argued that as other railway operators were willing to disclose similar specifications then UK operators should have no reason to withhold their specifications on the grounds that doing so would make ticket forgery more likely.

The Authority's submissions

21. The Authority confirmed that it held the information requested for the purposes of FOISA. However, it said that the information was in active control of RDG under their subsidiary, Rail Settlement Plan, on behalf of train operators.

22. The Authority noted that the Applicant had requested the following information:

    (i) the specifications for various ticket types, encompassing information about the creation of barcodes for rail tickets; and

    (ii) RSA keys/certificates, encompassing information about the decryption and translation of barcode information.

23. The Authority said that it anticipated disclosure of this information into the public domain, if misused, could result in the "creation, publication, and widespread dissemination of counterfeit barcodes, which could be used to enable ticket frauds". It argued that disclosure would therefore inhibit the prevention of widespread fraud and ticket counterfeit crimes and that this information being in the public domain, in turn, would significantly inhibit the detection and prosecution of such crimes.

24. The Authority also said that disclosure of this information could "directly facilitate fraudulent activity", which could lead to financial losses to railway operators and cause tangible and significant disruption to the Authority's services. It confirmed that it arrived at this view following expert opinion that had been shared with it by other industry partners on the security risks associated with disclosure of this information.

25. The Authority explained that the systems it was seeking to protect from disruption and fraud were highly technical in nature. It argued that if one technical aspect of these systems was entered into the public domain, then the risk of fraud applied not only to the other aspects of the systems but that there was also a real and substantial threat to all members of the Rail Settlement Plan (which included all major railway operators throughout the UK).

26. The Authority also noted that it had come to its attention that dedicated online communities exist whose purpose is to decode and reverse engineer the wider cryptographic ticketing systems, which it felt added to the substantial and real risk that it considered would follow from disclosure of the information requested.

27. The Authority also referred to a decision by the UK Information Commissioner[3] (UK ICO) that related to the same request as in this case, but which was made to London North Eastern Railway (LNER). It noted that, in this case, LNER had identified a case of fraud in Germany where a private key entered the public domain through a cyber-attack and bad actors created widespread fraudulent tickets before being identified. As the public keys were already available, this completed everything bad actors needed to proliferate the fraud throughout the Deutschlandticket system.

[3] https://ico.org.uk/media2/wcygt12z/ic-354648-y3l4.pdf

28. The Authority was asked to respond to the Applicant's argument that they had obtained equivalent information (that resulted in "no detriment" to the security of rail ticketing in the European Union) and that the information requested in this case should, therefore, also be disclosed.

29. The Authority said that it was not in a position to know, find out or confidently assess if the information disclosed by the European Agency for Railways was the same as that it was withholding from the Applicant. However, it again pointed to the UK ICO's decision in relation to LNER on this same question, where LNER relied on the fact that the EU standards are high-level and do not include UK-specific systems or the actual logic used within logic devices for validation. It also suggested that it did not appear to be "entirely true" that no detriment had resulted from disclosure of similar information in the European Union, as there had been "notable fraud ticketing schemes and investigations in the European Union as it is an inherent part of the business".

30. The Authority also made clear that the advice that it had received from RDG, as technical experts on these matters, was that the disclosure of the information requested would create a real and substantial threat to the safety of the Authority's ticketing systems. It shared with the Commissioner, for the purposes of his investigation, the advice it had received from RDG.

The Commissioner's view

31. The Commissioner has considered carefully all of the Applicant's and Authority's submissions, as well as the information withheld under the exemption in section 35(1)(a) of FOISA. He has also had regard to the advice that the Authority received from RDG.

32. The Commissioner also acknowledges the example the Authority referred to in the UK ICO's decision of the fraud and ticket evasion perpetrated in Germany, where certain technical specifications were publicly available and a key stolen, which enabled criminals to create fake but valid tickets.

33. The Commissioner notes that disclosure of information under FOISA is, effectively, disclosure into the public domain, and not just to the individual requesting the information. While the Applicant's motive for seeking the information may be reasonable, they are not the only individual to whom information would be accessible, were it disclosed in response to an information request.

34. Having taken all of the above factors into account, the Commissioner accepts the Authority's argument that the withheld information, if disclosed, could (and would be likely to) be used by individuals, so intent and with the requisite interest and expertise, to successfully create fraudulent tickets and to evade detection for criminal activity.

35. In all of the circumstances, the Commissioner is therefore satisfied, on balance, that disclosure of the withheld information would, or would be likely to, prejudice substantially the prevention or detection of crime to the extent that the exemption in section 35(1)(a) of FOISA is engaged. He will now go on to consider the public interest test in section 2(1)(b) in relation to the withheld information.

Public interest test

36. As noted above, the exemption in section 35(1)(a) is subject to the public interest test required by section 2(1)(b) of FOISA.

The Applicant's submissions on the public interest

37. The Applicant said that they believed there was legitimate scope for the withheld information, if disclosed, to be used in the public interest. For example, they suggested that it could be used in an application allowing automated expense reports from scanning train tickets or for adding train journeys to a personal itinerary planner.

38. The Applicant also argued that withholding these specifications allowed the Authority and other rail operators to "restrict the use of this data, whilst holding a (regulated) monopoly position on train services."

The Authority's submissions on the public interest

39. The Authority considered that the assessment of the public interest test it carried out at review stage still applied. As part of that assessment, it identified several factors that favoured disclosure of the withheld information, namely transparency, public trust and scrutiny, and technical understanding and innovation. However, it concluded that the risk of counterfeiting and increased security measures that would need to be implemented it the withheld information were disclosed, alongside "the increased pressure on public money use", meant that it was not in the public interest to disclose the withheld information.

40. The Authority maintained that the public interest was firmly in favour of not disclosing the withheld information based on several factors, which included the fact that withholding the information "would prevent any potential prejudice against police investigations and would reduce the strain on resources if the information is misused." Moreover, it considered that disclosure could help assist criminal activity through lowering the threshold to create fraud in the industry, which would make detection (of crimes such as ticket fraud) more difficult.

41. The Authority also said that revenue losses, alongside its commercial integrity, would be greatly affected if the information released resulted in fraudulent activities – "both in corporate image and in increased legal costs to combat this." In addition, it reiterated that the risk of counterfeiting and increased security measures that would be required if the information were disclosed would increase pressure on public money use.

42. The Authority considered that the technical nature of the information requested would not offer the public enough benefit to outweigh the potential harm of disclosure. It argued that technical insights into the way the ticketing system works would prove no benefit to equal access to its services or tangible improved understanding for the public and that it would only provide limited transparency to the public debate on the usage of public funds. As the withheld information is solely based on the technical aspect and not that of the costs or structures, it submitted that it could not be said that disclosure of this information would outweigh the harm.

The Commissioner's view

43. The Commissioner has considered the submissions from both the Applicant and Authority in relation to where the balance of the public interest lies.

44. The Commissioner acknowledges that there is a general public interest in openness and transparency in information held by public authorities. He accepts that disclosure of the withheld information would allow public scrutiny of that information. He also acknowledges that there may be a specific subsection of the population who could, if it were disclosed, use the withheld information constructively (in the manner suggested by the Applicant).

45. FOISA does not define the public interest. It has been defined elsewhere as "something which is of serious concern and benefit to the public", not merely something of individual interest. In other words, it serves the interests of the public.

46. While disclosure may be of interest to a specific subset of the population who have a particular interest in the technical nature of this information, this is not the same as disclosure serving the interests of the public.

47. In this case, the Commissioner has accepted that disclosure of the remaining withheld information would be likely to increase the production and use of fraudulent (but valid) rail tickets and thereby prejudice the prevention and detection of crime. This would not be in the public interest, nor would the financial implications of increased fraudulent tickets.

48. In all of the circumstances, the Commissioner is therefore satisfied that the public interest in maintaining the exemption in section 35(1)(a) of FOISA would outweigh any public interest in disclosure of the information.

49. The Commissioner is therefore satisfied that the Authority was entitled to withhold the information on the basis that the information was exempt information under section 35(1)(a) of FOISA.

Decision

The Commissioner finds that the Authority complied with Part 1 of the Freedom of Information (Scotland) Act 2002 in responding to the information request made by the Applicant.

Appeal

Should either the Applicant or the Authority wish to appeal against this decision, they have the right to appeal to the Court of Session on a point of law only. Any such appeal must be made within 42 days after the date of intimation of this decision.

Euan McCulloch
Head of Enforcement

24 October 2025