Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **3 March 2016**

Public Authority: **Bank of England**
Address: **Threadneedle Street**
London
EC2R 8AH

Decision (including any steps ordered)

1. The complainant submitted a request to the public authority for the number of cyber security incidents at the authority, the total number of times that the authority had engaged named specialist cyber security firms, and the total amount spent on their services, over a specified period.

2. The Commissioner's decision is that; in relation to Part 1 of the request, the public authority was entitled to rely on section 31(3) FOIA as the basis for not complying with the duty to confirm or deny whether it held the information requested. The public authority was also entitled to withhold information within the scope of Part 2 of the request on the basis of the exemption at section 31(1)(a) FOIA.

3. No steps are required.

Background, request, and response

4. On 2 April 2015 the complainant submitted the following request for information to the public authority:

'*Please provide details of any and all cyber/online security breaches at the Bank of England between 2010 and the present day, including: The total number of incidents broken down by year (eg 2012: 43); the nature of each incident (eg May 2014: malware infection); and the impact of each incident on the bank's operations. Such incidents include but are not limited to: denial-of-service attacks; malicious software detected on the bank's computers, network or computer systems; unauthorized access by an external actor to the bank's computers,*

network or computer systems; unauthorized access by a non-bank employee to the bank's internal email system; the theft of data or information stored electronically by the bank; detection of an unauthorised actor within the bank's internal network; any conduct by a bank employee that resulted in a breach of its online security.

Please provide details of each instance of the Bank of England's use of external cyber/online security firms since 2010, including: the date the firm was appointed, the nature of the work undertaken by the firm, and the sums paid to the firm for that work.'

5. The public authority originally denied the request in reliance on the exemption at section 31(1)(a) FOIA (Law Enforcement).

6. The complainant appealed the public authority's decision to the Commissioner. However, during the course of the Commissioner's investigation, the authority submitted that the cost of identifying, locating and retrieving the information in scope would in fact exceed the appropriate limit, and consequently sought to rely on the relevant provision in section 12 FOIA.[1] It however maintained the view that the information in scope would in any event be exempt from disclosure on the basis of section 31(1)(a), and possibly section 24(1) FOIA (National Security).

7. The Commissioner concluded that the public authority was entitled to rely on section 12(1) and explained this to the complainant who did not request a decision notice.[2] The case was subsequently closed.

8. The complainant subsequently wrote to the public authority on 3 August 2015 and submitted a narrower request in the following terms:

9. '*Part 1: Please provide figures for number of cyber/online security incidents at the Bank of England between 2010 and the present day that fell under the bank's most serious category of incident, for instance that invoked the Major Incident Management process. Broken down by year back to 2010.*

[1] By virtue of section 12(2), a public authority is not obliged to comply with a request for information if the authority estimates that the cost of complying with the request would exceed the appropriate limit.

[2] The Commissioner's decision would have remained the same regardless. The only difference is that a decision notice such as this one would have given the complainant the right to appeal the decision to the Information Rights Tribunal.

Part 2: Since 2010 how many times has the Bank of England used the following external firms for cyber security services: Context Information Security Ltd., BAE Systems Applied Intelligence, MWR Infosecurity Ltd, NCC Group, Nettitude Ltd., Cyberis Ltd., FireEye. What was the total spend on those firms?'

10. The public authority provided its response on 1 September 2015. It refused to comply with the duty imposed on public authorities by section 1(1)(a) FOIA to either confirm or deny whether they hold information requested by an applicant. It considered that the authority was excluded from the duty to confirm or deny whether it held any information within the scope of the request by virtue of the exclusion at section 31(3) FOIA.

11. The complainant requested an internal review on 1 September 2015. He disagreed with the public authority's decision to rely on section 31(3).

12. On 29 September 2015 the public authority wrote to the complainant with details of the outcome of its review. The original decision was upheld.

Scope of the case

13. The complainant contacted the Commissioner on 6 October 2015 to appeal the public authority's decision to rely on section 31(3). The Commissioner has addressed the complainant's submissions in support of his appeal further below.

14. During the course of the Commissioner's investigation, the public authority withdrew its reliance on section 31(3) in respect of Part 2 of the request. It subsequently confirmed that it held information within the scope of that part of the request which it in any event considered exempt from disclosure on the basis of section 31(1)(a).

15. The public authority additionally relied on the exemption at section 24(1) in respect of the information held within the scope of Part 2, and additionally on the exclusion at section 24(2) in respect of Part 1 of the request.

16. The public authority advised the complainant of its revised position above on 4 December 2015 and 25 January 2016 respectively.

17. The scope of the Commissioner's investigation therefore was to determine whether the public authority was entitled to neither confirm nor deny whether it held information within the scope of Part 1 in reliance on the exclusions at sections 31(3) and 24(2), and to withhold

information within the scope of part 2 in reliance on the exemptions at section 31(1)(a) and 24(1).

Reasons for decision

Part 1 - Section 31(1)(3)

18. The relevant parts of section 31 state[3]:

1) 'Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice— …….

(a) the prevention or detection of crime……

3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).'

19. Section 1(1) FOIA provides two rights to applicants. They are:

a) The right to be informed in writing by the public authority whether or not it holds the information requested by the applicant, and

b) If so, the right to have that information communicated.

20. Both these rights are subject to exemptions also set out in the FOIA.

21. The right in section 1(1)(a) is commonly referred to as a public authority's "duty to confirm or deny" whether it holds information.

Public authority's submissions

22. The public authority's position is that complying with the duty to confirm or deny in relation to Part 1 of the request would be likely to prejudice the prevention or detection of crime.

23. The public authority has argued that confirming or denying whether it holds the relevant information within the scope of Part 1 would assist those who want to attack its IT systems. If the authority were to confirm or deny that it held the information requested for a particular year, it

[3] The full text of the exemption can be found here: http://www.legislation.gov.uk/ukpga/2000/36/section/31

would be revealing whether the crisis management team/critical incident framework had or had not been invoked in any particular year in relation to a serious cyber incident.

24. Disclosing that the public authority had invoked its crisis management team/critical incident frame work in any particular year would help an IT attacker to establish that its attack had been detected, in particular as the nature of the attack might be such that the attacker could conclude with reasonable certainty whether it was or was not the cause of the invocation. Similarly, disclosing that the authority had not invoked its crisis management/critical incident framework in any particular year would help an IT attacker to determine that its attack had not been detected. Both scenarios could provide attackers with a valuable insight into the public authority's level of resilience, thereby facilitating the commissioning or concealment of crime in relation to fraud, data protection, terrorism etc.

25. The public authority added that it was aware external surveillance goes on all the time, with every small detail, including the kind of information sought by the complainant, potentially adding up, (through existing and/or prospectively available information whether gathered lawfully or not), to complete a picture for potential attackers and give clues as to the nature of the authority's systems, its likely defences and possible vulnerabilities.

26. It explained that its concern in this respect also ties in with recourse to information which the public authority might subsequently be required to disclose – so called mosaic or precedent effects - if it was to comply with this request. It argued that if the authority were required to comply with this request, this would clearly set a precedent for future cases and, at least, make it more difficult to refuse information in similar cases in future. In turn, if the public authority were to routinely disclose information in this domain, this would clearly facilitate an attacker's ability to link its own activities to those of the authority.

27. It submitted that the likelihood of prejudicing the prevention or detection of crime if it issued a confirmation or denial in response to Part 1 is real and significant given the public authority's role as the central bank of the United Kingdom (UK) and its designation as part of the UK's critical national infrastructure. Furthermore, it faces advanced, persistent and evolving cyber threats from a variety of sources which call for extreme vigilance and continual re-assessment as to how most effectively to address, and to mitigate risks concerning, those threats.

Complainant's submissions

28. The complainant expressed strong reservations against the view that issuing a confirmation or denial response to his request would have a '*real and significant impact*' on the public authority's operations. He submitted that, if for example, the authority were to disclose that there were no critical level cyber security incidents in 2013, and two in 2014, nothing about that information '*would give real and significant help to an attacker'*. In his view, it may be the case that an attack was dealt with without the need for invoking the crisis management process, and so would not figure in the data, or it may be that the process was invoked, but the attacker could not possibly know which incident invoked it.

29. He noted that public discussion about cyber threats takes place all the time, and that information sharing plays a vital role in combating threats. He pointed out that the public authority has made public pronouncements about its Waking Shark and CBEST penetration tests in the financial sector, including details about how to choose a supplier.[4]

Commissioner's finding

30. The public authority has made extensive submissions to the Commissioner in support of its reliance on the exclusion from the duty to confirm or deny, and on the application of exemptions. For the avoidance of doubt, he has considered the submissions in full including those parts he does not consider appropriate, for confidentiality reasons, to reproduce in this notice.

31. The Commissioner is persuaded by the public authority's submissions in support of the application of section 31(3). He accepts that revealing whether the public authority holds or does not hold the number of serious cyber security incidents broken down by each year from 2010 to 2015 would pose a real and significant threat to the authority's operations, and consequently, the prevention or detection of crime.

32. Given the public authority's critical role to the economy of the UK, there is no doubt that it faces persistent and evolving cyber threats and attacks from those who wish to carry out criminal activities including fraud and cyber-terrorism, against the authority in particular, and the UK's economy generally. The crucial question of course is whether

---

4 http://www.bankofengland.co.uk/financialstability/fsc/Documents/procuringpenetrationtestingservices.pdf

merely revealing whether information is held or not held in relation to Part 1 would be likely to assist those who wish to carry out criminal activities. In the circumstances described by the authority, the Commissioner accepts that a determined attacker would find the confirmation or denial useful. It could, for example, reveal (through deductive reasoning) that certain cyber attacks emanating from the attacker or others might not have been spotted or were not deemed serious enough. Alternatively, it could also reveal that a particular attack might have been spotted. It is the sort of information that could be combined with other information available to an attacker or already in the public domain to, as the public authority has emphasised, give clues to the nature of its systems and likely vulnerabilities.

33. While the Commissioner does not share the view that compliance with this request would clearly set a precedent for future cases, he accepts that it would at least make it more difficult in principle to refuse information in similar cases in future. The public authority was therefore correct to consider the possibility of a mosaic effect – ie- that the information revealed (ie a confirmation or denial) in compliance with this request could be combined with other information already in the public domain, or with information the authority could be forced to subsequently reveal as a result, to target its operations.

34. The test in this case is not, as the complainant suggests, whether the information revealed (ie a confirmation or denial) would give real and significant help to an attacker. The test is whether the prejudice envisaged from complying with section 1(1)(a) is real and significant. In the circumstances of this case, the Commissioner accepts that compliance with section 1(1)(a) would be likely to assist a determined attacker, and consequently, that the risk to the public authority's IT systems as a result, is real and significant. Furthermore, he does not consider that public pronouncements by the public authority in relation to the nature of cyber threats it faces, and the resilience of its cyber security, diminish the significance of the prejudice it envisages would be likely to occur should it comply with section 1(1)(a) in relation to this specific request.

35. The Commissioner therefore finds that the public authority was entitled to engage section 31(3) in respect of Part 1 of the request.

Public interest test

36. The exclusion at section 31(3) is subject to the public interest test set out in section 2(1)(b) FOIA. The Commissioner has therefore considered whether, in all the circumstances of the case, the public interest in maintaining the exclusion from the duty to confirm or deny in section

31(3) outweighs the public interest in disclosing whether the public authority holds information within the scope of Part 1 of the request.

37. The complainant argues that there is a public interest in knowing the extent of the threat of cyber attacks against the public authority, on which he claims, little is known.

38. The public authority acknowledged that transparency and accountability are important public interest considerations regarding its approach to cyber security. It explained that in recognition of these public interest considerations, its annual report for 2015 provides details of its cyber programme[5]. It also acknowledged that there may be circumstances where it is necessary and appropriate to publicly disclose details of a particular incident. It however argued that confirming or denying whether the public authority holds the information requested would not, of itself, contribute in any material sense to the public's understanding of its approach to cyber security.

39. It submitted that there are significant countervailing public interest considerations in any event against confirming or denying whether the information requested is held by the public authority. It pointed out that there is a substantial public interest in protecting society from the impact of crime and not facilitating any steps which are likely to prejudice the prevention or detection of crime.

40. More specifically, the public authority argued that there is a substantial public interest in not jeopardising the authority's resilience to cyber threats given the likelihood of an attack and the authority's wide-ranging responsibilities as the central bank of the UK. There is also a substantial public interest in not jeopardising the authority's resilience to cyber threats given the significant, adverse economic repercussions, domestically and internationally, which could flow from unauthorised access to the authority's systems.

Balance of the public interest

41. The Commissioner agrees that there is a public interest in the public authority being transparent about, and accountable for, its cyber security programme. The public should be confident in the ability of the authority to protect itself, and by extension, a crucial part of the UK

---

5 http://www.bankofengland.co.uk/publications/Documents/annualreport/2015/boereport.pdf in particular pages 49 and 50.

economy from cyber attacks. The complainant has acknowledged that the public authority publishes a wide range of information about its IT systems including advice to the financial sector generally on how to choose an IT supplier.

42. However, as the complainant will no doubt agree, there is a significant public interest in not publishing information which might expose the public authority's operations to cyber attacks given the significant implications that could have on the wider economy. On that basis, the Commissioner accepts that in all the circumstances of the case, the public interest in maintaining the exclusion from the duty to confirm or deny at section 31(3) outweighs the public interest in disclosing whether the public authority holds the information requested.

43. The public authority was therefore entitled to refuse to comply with the duty set out in section 1(1)(a) on the basis of the exclusion in section 31(3). The Commissioner has not considered the applicability of the exclusion at section 24(2) in light of his decision regarding the authority's application of section 31(3).

Part 2 – Section 31(1)(a)

44. As mentioned, information is exempt on the basis of section 31(1)(a) if its disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Complainant's submissions

45. The complainant submitted that the specialist cyber security firms he selected are on a '*publicly available list on* [sic] *government approved cyber incident response firms.*' He explained that he had not asked the public authority to disclose what each firm has done, or how many times each firm was used, '*just the total spend and the total number of times the companies on the list were employed'*. He also stated that he would be '*willing to agree to a redaction of the names of the firms on the list so they weren't made publicly available.*'

Public authority's submissions

46. The public authority pointed out that disclosing the information within the scope of Part 2 of the request would reveal that one or all of the named specialist cyber security firms had been engaged by the authority for cyber security services during the relevant period. It would also be providing some indication of the scale of the financial and business engagement with an important group of suppliers in the relevant period.

47. It argued that such information would reveal the extent of the public authority's engagement with such firms which could give some context

to the types of attacks experienced during the relevant period, thereby assisting in revealing whether cyber intrusion had been successful.

48. Furthermore, when combined with other intelligence, gathered lawfully or not, including information the authority could be forced to subsequently provide as a result (ie the mosaic effect), such information would be valuable additional intelligence to determined attackers. It would provide an attacker with valuable insight into the public authority's security posture, its level of resilience and its perceived strengths and weakness. For example, it would make it easier for attackers to determine what kind of defensive measures were in place, where the authority's weakness might be and the likely identity of contractors working in or with the authority. It would also provide useful detail enabling determined attackers to craft spear-phishing emails purporting to come from trusted firms and individuals and seek to infiltrate the relevant firm(s) for nefarious purposes.

49. It argued that the threat was real and significant given the public authority's role as the central bank of the UK and its designation as part of the UK's critical national infrastructure. Furthermore, as mentioned, it faces advanced, persistent and evolving cyber threats from a variety of sources which call for extreme vigilance and continual re-assessment as to how most effectively to address, and to mitigate risks concerning, those threats.

50. In response to the complainant's assertion that the seven named firms are on a publicly available list of government approved cyber incident response firms, the public authority explained that the Centre for the Protection of National Infrastructure (CPNI) and GCHQ had certified certain incident response firms and that possibly three of the seven firms are or were included on that list[6]. It however argued that it would be wholly misleading to infer from any such list that these are the only firms which might reasonably be expected to have been used by the public authority in relation to cyber security services.

Commissioner's finding

51. The Commissioner has considered the withheld information which as the complainant says, is primarily the total number of times the named firms were used by the public authority in the relevant period, and the total amount spent on the services rendered by the firms used. He agrees with the complainant that in and of itself the withheld

[6] http://www.cpni.gov.uk/advice/cyber/cir/

information seems wholly innocuous. Nevertheless, he is persuaded by the reasons given by the public authority in support of the application of the exemption to the withheld information.

52. He accepts that a determined attacker could use the withheld information in conjunction with other information already available to the attacker, in the public domain, or subsequently disclosed as a result of compliance with this request, to gain valuable insight into the perceived strengths and weakness of the public authority's IT systems. Revealing the extent and scale of the authority's engagement with specified specialist cyber security firms would be useful to a determined attacker who is gathering information in order to form a probable assessment of the authority's cyber security posture. Given that it is undoubtedly a prime target for those who wish to carry out criminal activities including against the wider UK economy, the withheld information in the wrong hands poses a real and significant risk to the public authority's operations, and consequently to the prevention or detection of crime.

53. The Commissioner does not consider that redacting the names of the selected specialist cyber security firms is a feasible option in the circumstances. Given that the request is about the public authority's engagement with firms who have been clearly identified, it is unclear how the withheld information would not be linked to them in the circumstances. The complainant already knows that the withheld information relates to the firms in question, not revealing their names would not change that fact.

54. The Commissioner therefore finds that the public authority was entitled to engage the exemption at section 31(1)(a).

Public interest test

55. The exemption at section 31(1)(a) is subject to the public interest test set out in section 2(2)(b) FOIA. The Commissioner has therefore considered whether, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the withheld information.

56. The complainant argues that the withheld information would serve the public by helping people understand how serious cyber security threats are, and by providing information on the public authority's expenditure to counter the threats.

57. The public authority's conclusions on the assessment of the balance of the public interest essentially replicate those previously set out in relation to the application of section 31(3).

Balance of the public interest

58. The Commissioner has carefully considered both the complainant's and public authority's submissions on the balance of the public interest. He is satisfied that, there is a significant public interest in not disclosing the withheld information in view of the real and significant risk to the public authority's IT systems and the UK's economy. On that basis, he has concluded that there is a significant public interest in maintaining the exemption.

59. The public authority was therefore entitled to rely on the exemption at section 31(1)(a). The Commissioner has not considered the applicability of the exemption at section 24(1) in light of his decision regarding the authority's application of section 31(1)(a).

Right of appeal

60. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0870 739 5836
    Email: GRC@hmcts.gsi.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

61. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

62. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Terna Waya
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF