The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

10 December 2024

IC-343234-K5N1

Request

You asked us:

"1) What is the current status of the investigation into the cyber attack on Arnold Clark which resulted in a data breach?
2) What information has been provided to the ICO by Arnold Clark in relation tothe circumstances of the cyber-attack and access to its customer data?
3) On what date did the breach occur, on what date was the breach discovered and on what date was it self disclosed to the ICO ?
4) What information has the ICO gathered about the nature of the breach anddata affected? Was the breach due to "human error" or inadequate cyber security measures as a consequence of inadequate investment ?
5) What information has been provided to the ICO by Arnold Clark in relation to the measures taken to secure customer data prior to the breach?
6) What information has been provided to the ICO by Arnold Clark in relation to the measures taken to recover and secure customer data after the breach?
7) Has the ICO reached any conclusions about the adequacy of Arnold Clark's security measures? If so, what conclusions have been reached and why?
8) Has the ICO uncovered any information which indicates that previous similar breaches of cyber security have occurred ? If so when, on how many occasions and what measures were taken to mitigate risk at these times ?
9) Is it confirmed that Arnold Clark has breached its data protection obligations and if so, which particular obligations, and why the ICO believes this to be the case.
11) Details of any action taken against Arnold Clark
12) Details of any advice (corrective or otherwise)given to Arnold Clark. Does any advice have timescales for implementation of measures applied
13) Any correspondence between the ICO and Arnold Clark, including; its initial self-report, cyber investigation report and all other materials supplied by Arnold Clark to the ICO.
14) If the investigation is ongoing, what are the timescales for conclusion?"

We received your request on 11 November 2024.

We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

I can confirm that we hold some information which falls within the scope of your request.

The investigation into the breach you refer to in your request was closed on 12 April 2024. The outcome was recorded as 'Advice provided'. This answers points 1 and 11.

Arnold Clark have publicly disclosed that the breach took place on 23 December 2022. The ICO received a breach report from Arnold Clark on 27 December 2022. This is the information we can disclose in relation to point 3.

Information which was provided to us by Arnold Clark is exempt under section 44 of the FOIA, in reliance upon section 132 of the Data Protection Act 2018 (DPA18). This includes information which falls within the scope of points 2-6 and 13. This exemption is explained further below.

Information relating to the investigation which was not provided to us by Arnold Clark is exempt under section 31 of the FOIA. This includes information which falls within the scope of points 4, 7, 9, 12 and 13. This exemption is explained further below.

We do not hold any information which falls within the scope of part 8 of your request. As the investigation is closed point 14 is not applicable.

Section 31 FOIA

Some of the information you have requested is exempt from disclosure under section 31(1)(g) of the FOIA. We can rely on section 31(1)(g) of the FOIA where disclosure:

"would, or would be likely to, prejudice… the exercise by any public authority of its functions for any of the purposes specified in subsection (2)."

In this case the relevant purposes contained in subsection 31(2) are 31(2)(a) and 31(2)(c) which state:

"(a) the purpose of ascertaining whether any person has failed to comply with the law…
(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise …"

Section 31 is not an absolute exemption, and we must consider the prejudice or harm which may be caused by disclosure. We also have to carry out a public interest test to weigh up the factors in favour of disclosure and those against.

We believe that disclosure of the information you have requested would be likely to damage the ICO's relationship with Arnold Clark and other data controllers. Being seen to disclose information without consent from the data controller involved is likely to result in them being reluctant to engage with the ICO in the future and would impact how other data controllers choose to engage with us. These relationships are essential in order for the ICO to improve data protection practices. Disclosure would therefore be likely to limit our ability to protect UK data subjects in the future in line with our regulatory duty.

In this case the public interest factors in disclosing the information are:

- increased transparency in the way in which Arnold Clarke has responded to the ICO's enquiries; and
- increased transparency in the way in which the ICO conducts its investigations.

The factors in withholding the information are:

- the public interest in the ICO providing a cost effective and efficient regulatory function. This relies on the cooperation of data controllers and we feel this is best achieved by an informal, open, voluntary and uninhibited exchange of information with these organisations. We feel that the cooperation of data controllers may be adversely affected if all details that they provide us, and our correspondence with them, were routinely made public. This would be likely to make data controllers more cautious about providing information to us which would in turn prejudice the ICO's ability to deliver the levels of service required of it;
- the public interest in maintaining the ICO's ability to conduct investigations effectively; and
- the public interest in data controllers being open and honest in their correspondence with the ICO about the way they have handled personal data, without fear that their comments will be made public prematurely or as appropriate at all.

Having considered all of these factors we have taken the decision that the public interest in withholding the information outweighs the public interest in disclosing it.

We note your comments about the use of section 31 to withhold this type of information. As explained above, in order to provide an efficient and effective

regulatory function we rely on data controllers engaging with us openly about their data protection practices and any breaches they may have experienced. Although we do have powers which can compel a data controller to provide us with the information we require this is time consuming and is not the best way to use our resources.

We have disclosed the fact that we have undertaken an investigation and provided the outcome type. Arold Clark have also made a public statement. Since no enforcement action was taken by the ICO we do not believe that it is in the public interest to disclose the detailed information you have requested. We are satisfied that withholding this information under section 31 of the FOIA is appropriate.

Section 44 FOIA

Information provided to us by Arnold Clark has been withheld under the provisions of section 44 of the FOIA which places prohibitions on disclosure. This exemption is an absolute exemption, which does not require a consideration of the public interest test of the type required by the qualified exemptions.

Section 44(1)(a) states:

"(1) Information is exempt information if its disclosure (otherwise than under this Act) by the public authority holding it -

(a) is prohibited by or under any enactment"

The enactment in question is the Data Protection Act 2018. Section 132(1) of part 5 of that Act states that:

"A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—

(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,

unless the disclosure is made with lawful authority."

Section 132(2) lists circumstances in which a disclosure can be made with lawful authority, however none of them apply here. As a result, the information is exempt from disclosure.

We can confirm that:

- The information was provided to the Commissioner in order to carry out their functions.
- The information relates to an identifiable business, specifically Arnold Clark.
- The information is not, and was not previously, publicly available from other sources.

As a result we cannot disclose the information unless we have lawful authority.

Section 132(2) of the DPA provides conditions in which disclosure could be made with lawful authority. We have therefore considered each condition in turn:

"(a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business,"

We can confirm that we do not have consent to disclose this information.

"(b) the information was obtained or provided as described in subsection (1)(a)for the purpose of its being made available to the public (in whatever manner),"

The information was not obtained by or provided to the Commissioner as part of their regulatory role in order to make it available to the public and for this reason we are treating it as confidential.

"(c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner's functions,"

We find that disclosure is not necessary in order to fulfil any of their functions.

"(e) the disclosure was made for the purposes of criminal or civil proceedings, however arising,"

Disclosure would not be for the purposes of criminal or civil proceedings.

"(f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest."

We do not consider it necessary or justifiable to disclose this information as there is no compelling public interest to do so. The Commissioner and his staff risk criminal liability if they disclose information without lawful authority. The right of access under the FOIA is not sufficient to override these important factors and the information is therefore withheld.

This concludes our response. We appreciate that this may be disappointing given your comments on the public interest in disclosure of this information. However, we hope we have explained our decision clearly.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full review procedure on our website.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can raise a complaint through our website.

Your information

Our privacy notice explains what we do with the personal data you provide to us, and sets out your rights. Our Retention and Disposal Policy details how long we keep information.

Yours sincerely

Information Access Team
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews