

12 January 2024

Case reference: IC-278284-Y0F9

We are now in a position to respond to your information request of 22 December 2023.

Request

*"Freedom of Information (Scotland) Act
Arnold Clark data breach investigation*

We refer to the above and make a request under the Act for information relating to the Information Commissioner's investigation into the breach of customer data held by Arnold Clark in a cyber security incident on 23 December 2022. We understand that this breach was reported and an investigation commenced.

- 1) What is the current status of the investigation?*
- 2) What information has been provided to the ICO by Arnold Clark in relation to the circumstances of the cyber-attack and access to its customer data?*
- 3) What information has the ICO gathered about the nature of the breach and data affected?*
- 4) 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?*
- 5) 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?*
- 6) Has the ICO reached any conclusions about the adequacy of Arnold Clark's security measures? If so, what conclusions have been reached and why?*
- 7) If the investigation is ongoing, what are the timescales for conclusion?*

Should there be any further information available in relation to the investigation and/or steps taken as a result of the breach, we would be grateful if this could also be provided."

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

Our response

We note you have mentioned the Freedom of Information (Scotland) Act 2002. The information we hold within scope of your request is held in our capacity as regulator of data protection legislation, which covers the whole of the UK.

Our investigation into this data security incident is ongoing. Having liaised with the relevant team, we are not able to provide a timescale for its conclusion at this time.

With regards to the remaining requests in points 2 to 6 and your final point, we are withholding this information under sections 31 and 44 of the FOIA and further details on these exemptions are provide below.

Section 31(1)(g) FOIA

Section 31(1)(g) of the FOIA states:

'Information... is exempt information if its disclosure under this Act would, or would be likely to, prejudice – (g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2)'

The purposes referred to in sections 31(2)(a) and (c) are:

- 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

The purposes at section 31(2)(a) and (c) apply when a regulator is determining whether or not there has been a breach of relevant legislation, and whether any further action is appropriate.

The exemption at section 31 is not absolute, and we need to consider the public interest test by weighing up the factors for and against disclosure of the information we hold at this time, as well as any prejudice or harm which may be caused by disclosure.

Our investigation into these matters is ongoing. To release the information you have requested at the present time could prejudice the ICO's ability to conduct the investigation fairly and in an appropriate manner.

In considering the prejudice and/or harm that disclosure may cause, we have taken into account the factors that would, in our view, impact on the release of the requested information at this time. We have considered the public interest test for and against disclosure.

In this instance, the public interest factors in favour of disclosure are:

- Openness and transparency in the way in which the ICO conducts its investigations of the data security incidents reported to us.
- The understandable interest of the public, and any data subjects affected, in being able to see and understand the precise nature of this incident.

The public interest factors in favour of maintaining the exemption are:

- The need for the ICO to continue to encourage Arnold Clark Automobiles Ltd, and other data controllers, to engage with us as regulator in the investigation of data security incidents.
- To allow the ICO to maintain the trust and confidence of data controllers by affording the information provided an appropriate level of confidentiality. Disclosure of information provided in confidence, or considered confidential, would be likely to have a long term detrimental effect on the self-reporting of incidents and our ability to investigate them.
- Allowing us a 'safe space' in which to consider the information gathered, free from external influence, and to ensure the confidentiality of the enquiries undertaken, information provided, and analysis of the incident in question.
- The ICO has a demonstrable history of sharing information about our enforcement and regulatory activities when it is appropriate to do so, in line with our 'Communication our regulatory and enforcement activity policy'. Available online [here](#). We publish details of the action we take on our website [here](#).

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.

Section 44 FOIA

Section 44 of the FOIA is an absolute exemption which means that it can be withheld without further consideration if other legislation prevents its release, if it meets certain conditions, and if none of the circumstances that would give us lawful authority to release it apply.

Section 44(1)(a) of the FOIA 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'

In this case, the Data Protection Act 2018, part 5, section 132 prohibits the disclosure of confidential information that –

- 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.

We do not have lawful authority to disclose to you the information relating to the data security incident reported by Arnold Clark Automobiles Ltd as this information was provided to us in confidence.

Section 132(3) imposes a criminal liability on the Commissioner and his staff not to disclose information relating to an identifiable individual or business for the purposes of carrying out our regulatory functions, unless we have the lawful authority to do so or it has been made public from another source.

This concludes our response to your request. We understand this response may be disappointing but hope the information provided above is helpful.

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 [here](#).

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
Risk and Governance Department, Corporate Strategy and
Planning Service
Information Commissioner's Office, Wycliffe House, Water
Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews

**For information about what we do with personal data
see our [privacy notice](#)**