The ICO exists to empower you through information.

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

24 July 2024

IC-318757-D5S4

Request

You asked us:

Is it possible to confirm whether the ICO is working with the FBI on an investigation into Ticketmaster?

They company was charged with 5 charges including computer intrusion for commercial advantage or private financial gain: for hacking into the database of a rival company from 2012-2015. In 2020, Ticketmaster was fined £10m and had to report to the United States District Court in New York in a delayed prosecution deal – part of which included Ticketmaster's cooperation with foreign law enforcements and regulatory bodies.

The victim company was British (SongKick) and one of the Ticketmaster employees was also British.

Is it possible to also confirm any other data breaches Ticketmaster has been investigated over with the ICO please?

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

Response

We hold information about two personal data breach cases involving Ticketmaster. We have published information about one of these here:

Ticketmaster UK Ltd MPN

In the case of the other, we have received a report and are currently making enquiries but are unable to confirm any further details while the issue is still live.

Therefore we can neither confirm nor deny whether the ICO is working with the FBI on an investigation involving Ticketmaster, nor can we confirm nor deny whether the matter we are currently investigating is linked to any of the details provided in your request, by virtue of section 31(1)(g) and section 31(2)(c) of the FOIA. The reasoning for this is explained below.

Section 31(3) states;

"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)."

Section 31(1)(g) provides that *"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 the exercise by any public authority of its functions for any of the purposes specified in subsection(2)"*

Confirming or denying whether this information is held would prejudice the purpose specified at section 31(2)(c) of the FOIA, namely *"the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise,"*

We believe that prejudice would be likely to arise because confirming or denying details relating to the current investigation at this time would be likely to prejudice that investigation, regardless of whether any formal regulatory action is ultimately taken.

We take the view that to confirm or deny these details could prejudice the ICO's ability to conduct the investigation in an appropriate manner. For example, it is probable that confirming or denying any details at this stage would discourage discussions between the ICO and any parties involved, and may damage our ability to conduct and conclude the investigation fairly and proportionately.

Confirming or denying specific details about our investigation could also jeopardise the ICO's ability to obtain information either relating to this case or others in the future. In our view harm could be caused if other parties were reluctant to enter into any further discussions if details had already been confirmed or denied in response to information requests or even general enquiries. This is likely to result in other parties being reluctant to engage with the ICO in the future. In addition, confirming or denying any details at this stage could be misinterpreted, which in turn could distract from the investigation process.

We are therefore satisfied that there would be prejudices associated with confirming or denying details about the current investigation.

We have also considered the following public interest arguments in favour of confirming or denying whether the information is held and in favour of maintaining the exclusion from the duty to confirm or deny.

Public interest arguments in favour of confirming or denying:

Confirming or denying whether the requested information is held would allow the public to increase its understanding of the parameters of the investigation and therefore increase transparency and accountability in relation to our regulatory activities. This is particularly relevant for any data subjects that may have been affected.

Public interest arguments in favour of maintaining the exclusion from the duty to confirm or deny:

It is in the public interest to maintain the integrity of an investigation and the effectiveness of our regulatory function whilst that investigation is ongoing. To publicise exactly what information we do or do not hold could subvert the investigative process and, consequently, its effectiveness.

Confirming or denying particular details about a live investigation is also likely to hinder the ICO's ability to conduct investigations as it sees fit, without undue external influence, which might affect our decision making or divert our resources in future.

There is public interest in organisations being open and honest in their correspondence with the ICO about the way they have handled a personal data breach, without fear that details about anything they report to us will be confirmed or denied prematurely or, as appropriate, at all.

It is key to our work that we can encourage organisations to proactively engage with us, report incidents, and go on to cooperate with any investigation.

The balance of the public interest

In this case, we find that the balance of the public interest is in favour of maintaining the exclusion from the duty to confirm or deny. For the ICO to disclose information which could prejudice an investigation, would undermine the integrity of the investigation and make the ICO a less effective regulator which is

not in the public interest.

We therefore find that the public interest in this case favours maintaining the exclusion from the duty to confirm or deny whether this information is held.

For the avoidance of doubt, nothing in this response should be taken to either confirm or deny the above requested information is held.

Advice and assistance

We publish information some about personal data breaches reported to us here as well as information about complaints, investigations and other casework. We also publish information about action we've taken, and summaries in our annual reports.

Please note that we do not retain information about personal data breaches indefinitely, and details are held in accordance with our retention policy.

Not all personal data breaches need to be reported to the ICO. For more information see our guidance here.

Requests for information relating to specific personal data breaches may be subject to exemptions, for example if these relate to live investigations or involve third party data.

This concludes our response to your request.

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
Strategic Planning and Transformation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews
Please consider the environment before printing this email