

Our ref **FOI 4649**

Rebecca Moody
request-805752-ce5fa835@whatdotheyknow.com

21 December 2021

Please write to Data protection team
Financial Ombudsman Service
PO Box 73208
London
E14 1QQ

DX 141280 Isle of Dogs 3
Website www.financial-ombudsman.org.uk

Sent by email only

Dear Rebecca Moody,

Your request for information

Thank you for your email of 11 November 2021, in which you asked for the following information:

"Please find below my FOI request regarding malicious emails sent to the department.

The date range for the requests is from 2018 to present day. The data shall include a breakdown by year and by individual departments (e.g. separate departments, agencies, or public bodies within the main government agency), if applicable.

- 1. How many malicious emails have been successfully blocked?*
- 2. What percentage of malicious emails were opened by staff?*
- 3. What percentage of malicious links in the emails were clicked on by staff?*
- 4. How many ransomware attacks were blocked by the department?*
- 5. How many ransomware attacks were successful?"*

Response

I've carefully considered your request and unfortunately, the information that you have requested is exempt under section 31 of the Freedom of Information Act (FOIA) which relates to Law Enforcement, and section 31(3) which removes the public authority's duty to confirm or deny whether information is held, if to do so would or would be likely to prejudice law enforcement.

Although you may have a genuine interest in the information requested, as you are aware FOIA responses are public information and can be made available to the world.

We have a duty to protect this information. To confirm or deny whether we hold this information about malicious emails and ransom ware attacks would provide actual knowledge that where an attempt has been made, it has or has not been successful. This information could compromise our information security systems and may assist individuals in the commission of a criminal offence by giving malicious actors insight into vulnerabilities which may, or may not, exist on our systems.

In applying this exemption, we have to balance the public interest in withholding the information against the interest in favour of disclosure. This public interest test is not about whether we should disclose any information that we might hold. It is a test of whether we should say if we hold the information or not.

Factors against neither confirming or denying:

- Confirming the information requested is held would help transparency and accountability of the Financial Ombudsman Service.
- Would provide information about effectiveness and resilience of our information security systems in withstanding cyber-attacks.

Factors favouring neither confirming or denying:

- Confirming the information requested is held would reveal how effective our security systems are and would likely give malicious actors insights into both the strengths of our cyber security posture and any potential weaknesses that may exist. This would prejudice the prevention of crime by increasing the chances of cyberattacks which are criminal offences. Cyber security measures are in place to protect the integrity of personal information, special category personal data and other sensitive personal information and increasing the chances of an attack would have potentially serious repercussions on individuals (including customer and employees of the service).
- Confirming that we hold limited information in this area could either show we have poor reporting and recording procedures which will encourage an attack, or it could show we have robust procedures which could encourage an attack to try out malicious actors new techniques.
- Complying with our legal obligations to keep personal data secure and to take appropriate measures which includes keeping areas confidential where necessary is in the public interest.

Whilst there is a strong public interest in the transparency of the Financial Ombudsman Service, we will not confirm or deny whether information is held, if it is likely that this will compromise our statutory functions or place members of the public at risk.

Having taken all the relevant factors into account, I've concluded that the public interest in maintaining the exemption outweighs the public interest in confirming or denying whether information is held. We can neither confirm nor deny whether this information is held.

I hope that my response addresses your request; but if you don't believe we've fully complied with the Freedom of Information Act 2000 the next steps are overleaf.

Yours sincerely,



Kevin Gauchan
Data protection and FOI adviser

Email data.protection@financial-ombudsman.org.uk

If you're not satisfied with our response

If you're unhappy with our response, please contact us within two months of the date of this letter – explaining why – and asking us to carry out a review. You can contact us by email at: data.protection@financial-ombudsman.org.uk

If you're still unhappy after we've carried out our review, you can contact the Information Commissioner's Office within three months. You can contact them at:

Phone	0303 123 1113
Email	casework@ico.org.uk
Website	https://ico.org.uk/make-a-complaint