



Our ref: LEX 1201

28 February 2023

C Drake

Email: [foi+request-9548-cbfc82e3@righttoknow.org.au](mailto:foi+request-9548-cbfc82e3@righttoknow.org.au)

Dear C Drake

**Freedom of Information Request – LEX 1201**

I refer to your request dated 10 November 2022 made under the *Freedom of Information Act 1982 (Cth)* (the Act) in the following terms:

*“Background: I request the details of cybercrime reports submitted to “Police” between and including July 2021 to June 2022 for the purposes of “analysing cybercrime data” with the aim of preventing this criminal activity through political consultation (educating elected representatives to the losses being suffered by their constituents, and proposing effective legislation to curb losses to these crimes).*

*I need at least enough detail to identify victim electorates, victim types, crime types, and as much information about losses as possible, for the 2021-2022 Financial Year.*

*Request: Statistics of matters referred to the AFP by the Report Cyber system for the 2021-2022 financial year.”*

The Commissioner of the AFP, being the principal officer of the agency, has authorised me to make decisions on behalf of the agency in respect of the Act.

Searches for documents were undertaken by the AFP’s Cyber Command. These searches identified 42 documents in scope of your request.

Section 7(2A) of the Act provides:

*An agency is exempt from the operation of this Act in relation to the following documents:*

*(a) a document (an **intelligence agency document**) that has originated with, or has been received from, any of the following:*

- (i) the Australian Secret Intelligence Service;*
- (ii) the Australian Security Intelligence Organisation;*
- (iii) the Inspector-General of Intelligence and Security;*
- (iv) the Office of National Intelligence;*
- (v) the Australian Geospatial-Intelligence Organisation;*

# OFFICIAL

- (vi) *the Defence Intelligence Organisation;*
- (vii) *the Australian Signals Directorate*

The document identified as being in scope of your request originated with an intelligence agency. Accordingly, the AFP is exempt from the operation of the Act in relation to the document. As such, the AFP will be taking no further action in relation to your request.

## **Additional Information**

To assist you with your further research, AFP Cyber Command has provided additional information regarding the reporting requirements and documents that are in the possession of the AFP.

ReportCyber is the main public cybercrime reporting mechanism for Australia. The AFP and State and Territory Police maintain their own investigational systems which are separate to ReportCyber. The ACSC manages ReportCyber and conducts analyses of ReportCyber reports and publishes annual reports, such as the recently released *2022 ACSC Cyber Threat Report*: <https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf>. The AFP notes that not all cases of cybercrime result in or involve fraud. This is reflected in the *2022 ACSC Cyber Threat Report*.

Reports submitted by members of the public are collected by the ACSC via ReportCyber and automatically referred to the relevant Australian policing jurisdiction. These reports are not referred to the AFP unless the victim is identified as a Commonwealth entity or another jurisdiction assesses that the matter should be re-referred to the AFP. The types of cybercrime the AFP responds to are predominantly those involving Commonwealth entities or information systems of national significance or where the incidents have the potential to impact the whole of the Australian economy. State and Territory Police have the lead in relation to cybercrimes against Australian individuals and businesses.

Page 22 of the *2022 ACSC Annual Cyber Threat Report* provides a breakdown of cybercrime reports by the state or territory law enforcement agency assigned to each report. From that chart, 100% of all reports were assigned to State or Territory police.

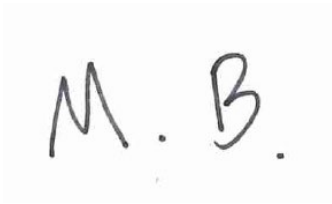
Of the over 76,000 reports received by ReportCyber for the financial year 2021 to 2022, 10 matters were referred or re-referred to the AFP where there was a financial loss recorded. As such, any statistics based on the matters referred to the AFP would not be “sufficient to accurately calculate reported loss values broken down by Australian electoral boundaries (or at least by postcode)”.

The AFP further notes the ACSC’s commentary on page 21 of the *2022 ACSC Annual Cyber Threat Report* in relation to the overall difficulty in accurately estimating the cost of cybercrime as self-reported financial loss data, as submitted to ReportCyber, only captures a small portion of the total financial impact.

OFFICIAL

**OFFICIAL**

Yours sincerely

A handwritten signature consisting of the letters 'M.' followed by a period, then 'B.' followed by a period, all in black ink on a light background.

Matt Baillie  
Principal Lawyer  
Freedom of Information and Privacy  
Chief Counsel Portfolio

**OFFICIAL**

# OFFICIAL

**\*\*\*YOU SHOULD READ THIS GENERAL ADVICE IN CONJUNCTION WITH THE LEGISLATIVE REQUIREMENTS IN THE FREEDOM OF INFORMATION ACT 1982\*\*\***

## **REVIEW AND COMPLAINT RIGHTS**

If you are dissatisfied with a Freedom of Information decision made by the AFP, you can apply for a review by the Information Commissioner (IC).

For complaints about the AFP's actions in processing your request, you do not need to seek review by either the AFP or the IC in making your complaint.

### ***REVIEW RIGHTS under Part VII of the Act***

#### ***Review by the Information Commissioner***

Section 54L of the FOI Act gives you the right to apply directly to the IC for review of this decision. In making your application you will need to provide an address for notices to be sent (this can be an email address) and a copy of the AFP decision.

Section 54S of the FOI Act provides the timeframes for an IC review submission. For an *access refusal decision* covered by section 54L(2), the application must be made within 60 days. For an *access grant decision* covered by section 54M(2), the application must be made within 30 days.

Applications for IC review may be lodged by email ([foidr@oaic.gov.au](mailto:foidr@oaic.gov.au)), using the OAIC's online application form (available at [www.oaic.gov.au](http://www.oaic.gov.au)) or addressed to:

Office of the Australian Information Commissioner  
GPO Box 5128  
Sydney NSW 2001

The IC encourages parties to an IC review to resolve their dispute informally, and to consider possible compromises or alternative solutions to the dispute in this matter. The AFP would be pleased to assist you in this regard.

#### ***Complaint***

If you are unhappy with the way we have handled your FOI request, please let us know what we could have done better. We may be able to rectify the problem. If you are not satisfied with our response, you can make a complaint to the IC. A complaint may be lodged using the same methods identified above. It would assist if you set out the action you consider should be investigation and your reasons or grounds.

More information about IC reviews and complaints is available on the OAIC's website at <https://www.oaic.gov.au/freedom-of-information/reviews-and-complaints/>.

OFFICIAL