Notifiable Data Breach Form

Statement about an eligible data breach

Organisation/agency details

You must complete this section

Organisation/agency name * Catholic Archdiocese of Sydney

Phone * 1800 898 396

Email * Privacy@sydneycatholic.org

Address Line 1 * Level 16, Polding Centre, 133 Liverpool Street

Address Line 2

Suburb * Sydney

State * NSW

Postcode * 2000

Other contact details

Description of the eligible data breach

You must complete this section

A description of the eligible data breach: *

On or around 26 August 2019, Catholic Archdiocese of Sydney (**CAS**) became aware that the Outlook mailbox of a CAS staff member (**Inbox**) had been accessed by an unauthorised third party or parties located overseas. The breach appears to have been caused by the relevant employee unwittingly clicking on a scam phishing email and followed by entering in their Outlook user credentials. These user credentials appear to have been used by the attacker to access the employee's Outlook via CAS' webmail application. The mailbox appears to have been accessed via CAS' webmail application between 13 and 20 August 2019, and approximately 20% of the Inbox (by size) was downloaded; it is impossible to determine which specific emails were downloaded and whether, and what, personal information stored on the Inbox had been accessed.

Upon becoming aware of the data breach, CAS took immediate steps to secure the Inbox to prevent further unauthorised access, including (a) isolating the affected user's workstation; (b) renewing the affected user's password; and (c) scanning the affected user's devices for malware or any indications of compromise.

Subsequently, CAS undertook extensive investigations into the circumstances surrounding access to the Inbox and the possibility of personal information being accessed. Among other things, the investigations revealed that the incident was unlikely to have been specifically targeted for malicious purposes towards CAS or affected individuals; rather, the incident was most likely carried out by an unsophisticated actor motivated by financial gain. Notwithstanding the passage of time since the incident, CAS has not been made aware of any evidence of misuse of any personal information that may have been the subject of the data breach.

Upon becoming aware of the incident, CAS promptly notified the Office of the Australian Information Commissioner, and has been engaging with them since. CAS has already directly notified certain specific groups of individuals that may possibly have been affected by the data breach. The purpose of this broader notification is to notify a broader set of affected persons whose personal information may have been included in the downloaded emails.

Information involved in the data breach

You must complete this section

Kind or kinds of personal information involved in the data breach:

In general terms, the kinds of personal information involved in the data breach includes individuals' first and last names, personal and business contact details (such as email address, home or business address and/or telephone or mobile number), bank details, employment history and current employment details, education history, health information (including information on mental health), and (if applicable) civil proceedings against CAS or one of its ministries, or allegations of crime or claims relating to individuals.

In addition, please select any categories that apply:

☒ **Financial details**

☒ **Tax File Number (TFN)**

☒ **Identity information**
(e.g. Centrelink Reference Number, passport number, driver license number)

☒ **Contact information**
(e.g. home address, phone number, email address)

☒ **Health information**

☒ **Other sensitive information (e.g. sexual orientation, political or religious views)**

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach: *

CAS recommend that individuals remain vigilant to the possibility of suspicious activity, particularly in the form of unwanted or unrecognisable communications from unknown telephone numbers and/or email addresses. Other options to help reduce the likelihood of receiving such communications include changing telephone numbers and/or email addresses where a personal email address was provided. Individuals can also contact the Office of the Australian Information Commissioner (1300 363 992) for further guidance on their rights under Australian privacy law.

Individuals can also contact CAS on 1800 898 396 which has been set up to respond to questions arising from this notification and the data breach. The hours of operation are 9am to 5pm Monday-Friday (except public holidays) AEST.

CAS is also undertaking a number of internal steps to reduce risk of future data breaches, including reviews of staff training and policies and procedures, implementing additional internal tools to report and improve email security and incident handling, and blocking connection attempts from geographic areas identified as high risk.

CAS takes the security of all personal information it collects and hold very seriously, and is committed to meeting Australian privacy law requirements to protect personal information and notify affected individuals of data security incidents.