FOOTBALL AUSTRALIA DATA BREACH
FREQUENTLY ASKED QUESTIONS

QUESTION	ANSWER
1. What happened?	Certain Football Australia cloud storage data repositories were inadvertently made publicly accessible due to a system misconfiguration (not malicious activity). That misconfiguration has been rectified. More specifically: • A file listing (that is, the names of files but not the contents of those files) for a data repository was accessed by an unauthorised third party, and certain data from this and an additional repository was publicly accessible at various intervals from April 2022 to February 2024. These two repositories (the ***FALeague repositories***) contained information about approximately 1,600 A-League Women, A-League Men and A-League Youth players, team personnel and, in a few cases, some of their family members. Not all of this information was present for all of those individuals. While Football Australia is not able to conclude with certainty that the data in those repositories relating to those 1,600 individuals was actually accessed by an unauthorised third party, we cannot rule this out. • A single file in a data repository relating to Football Australia match ticketing information for 234 individuals was accessed by an unauthorised third party (the ***ticketing file***).
2. What types of personal information were impacted?	The FALeague repositories contained the contact details, identity documents, financial information, and health information of approximately 1,600 A-League Women, A-League Men and A-League Youth players, team personnel and, in a few cases, some of their family members. Not all of this information was present for all of those individuals. While Football Australia is not able to conclude with certainty that the data in those repositories relating to those 1,600 individuals was actually accessed by an unauthorised third party, we cannot rule this out. The ticketing file contained names and contact details, as well as seating, ticket quantity and price information for 234 individuals. It did not include their payment details (other than method of payment such as Visa or Mastercard) or dates of birth.
3. How will I know if I have been impacted?	If you have been identified as being at sufficient risk as a result of the incident, Football Australia will notify you directly.
4. I have received a notification from Football Australia. How do I know if it is legitimate?	Please always check the sender of any communications purporting to be from Football Australia. We will never demand money from you or ask for your password. If you notice any communications or other activity purporting to be from Football Australia which causes you concern, please let us know immediately by contacting us at privacy@footballaustralia.com.au.
5. What can I do to protect myself?	We encourage you to always remain vigilant to scams by taking the following steps: • Always use strong, unique passwords for all your accounts (including any financial services accounts) and update them regularly. Do not reuse passwords across accounts and services and do not share your passwords with anyone. Enable multi-factor authentication for your accounts where it is available. • Be vigilant for suspicious behaviour, including on your online accounts and in any contact that appears to come from Football Australia. • Watch out for unexpected calls and texts, particularly if they ask for your personal information or refer you to a web page asking for your personal information. If you are ever concerned that a call may not be legitimate, end the call without providing your personal information and call back on a publicly listed number. Don't assume that a call is legitimate just because it appears to come from a publicly listed number, as scammers are able to mask their phone numbers to make them appear legitimate. • Report any harassing or threatening communications to the police. You can also report such messages to the Australian Cyber Security Centre's "ReportCyber" service here: https://www.cyber.gov.au/acsc/report. • Familiarise yourself with guidance on protecting yourself from scams. Remember that scammers may use information they already know about you in order to appear trustworthy. The Australian Scamwatch initiative offers guidance here.

Football Australia Ltd
ACN 28 106 478 068
Locked Bag A4071, Sydney South NSW 1235
Tel: +61 2 8020 4000 Fax: +61 2 8020 4100

	If you have received a notification from Football Australia, your notification will include additional information about what to do in relation to the specific types of personal information that may have been impacted.
6. Has any data from this incident appeared on the dark web?	The only personal information from this incident we are aware has been published online is an extract of a file listing (that is, the names of some files but not the contents of those files) for one of the FALeague repositories appearing on social media and news publications. We are not aware of any of the underlying contents of the FALeague repositories or the ticketing file being published on the dark web. Football Australia is continuing to undertake dark web and surface web monitoring.
7. How has Football Australia responded and how are you supporting affected individuals?	Football Australia is offering the following services to individuals that it notifies about the incident (at no cost to them): • Equifax credit and identity monitoring services • Specialist identity support services from IDCare, Australia's national identity and cyber support service. In addition, if your notification identifies that your government-issued identity document has been impacted and the relevant issuing agency has advised us that it recommends that the document be replaced, Football Australia will reimburse you for the cost of that replacement. Information about how to access these services and how to claim reimbursement (where applicable) will be included in your notification. Since becoming aware of the issue, we have: • Advised the Office of the Australian Information Commissioner (OAIC) and the Australian Cyber Security Centre (ACSC) of the matter and have been working with the Cyber Security Response Coordination Unit (CSRCU); • Initiated an external investigation into the issue; and • Enhanced the security of our data repositories. Football Australia has also been undertaking dark web and surface web monitoring.
8. Was the 'Play Football' participation registration portal affected by this misconfiguration?	No.
9. Why is Football Australia notifying individuals now?	We needed to investigate the issue and understand what happened and who it impacted. That takes time. The scope of impact was much more confined than initial media reports. To avoid causing unnecessary alarm or notification fatigue, it was important for us to be as clear as possible with our players, officials, and stakeholders about whether and how they had been impacted so that they could take meaningful action to protect themselves. Football Australia apologises to those affected by the incident, and we thank the football family for its patience as we investigated the matter. Since becoming aware of the issue, we have enhanced the security of our data repositories, and we continue to prioritise the privacy and confidentiality of our stakeholders' and customers' information.
For media enquiries contact: media@footballaustralia.com.au.	