

---

As was widely reported by news organizations, recently a [cyberattack](#) exploiting a flaw in a popular file-transfer software known as MOVEit affected hundreds of organizations worldwide, including a number of federal agencies and contractors.

One organization affected was the National Student Clearinghouse (NSC). NSC provides educational reporting, data exchange, verification, and research services to many higher education institutions, including American National University for a short period during 2018 and 2019. In connection with such services, ANU shared information on prospective and current students, including such students' social security numbers, but not including any financial account information. NSC has posted information about this incident to the NSC website, including answers to questions [here](#). General information about NSC's published data privacy and security practices can be found on the NSC website [here](#).

On August 15, 2023 NSC informed ANU of the results of its investigation into the data breach and the affect on ANU students:

“The investigation revealed that an unauthorized third party obtained certain files transferred through the MOVEit software, including files containing personal information that the Clearinghouse maintains on behalf of our customers. The affected files were then analyzed to determine the individuals whose personal information appeared in the files and the data providers who submitted that information to the Clearinghouse. In some of the affected files, personal information such as Social Security numbers, student identification numbers, or dates of birth appeared. However, the individuals identified [as students at American National University] did not have a Social Security number, student identification number, or date of birth from your organization appearing in the affected files. For the individuals identified [as students at American National University], the types of affected personal information may include names, contact information, and educational information such as enrollment, degree, and course-level data (for example, from transcripts and Postsecondary Data Partnership reports), although the types of information vary by individual.”

Although NSC advised that no individual notification to affected ANU students would be made in view of the limited scope of ANU students' personally identifiable information compromised by the breach (no Social Security numbers, student identification numbers, or dates of birth), ANU recommends that students who were in attendance at ANU during 2018-2019 closely monitor their financial accounts for [suspicious activity](#). You can also [check your credit report for free](#) and, if necessary, consider placing a [credit freeze](#) on your credit report with each of the three credit reporting agencies.