

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Incident Response](#)



## Personal Information of Over 30,000 Students Exposed in Unprotected Database

By [Ionut Arghire](#) on June 06, 2022

Share

Tweet

推荐 13



The personal information of more than 30,000 students was found on an improperly secured Elasticsearch server, security researchers with SafetyDetectives report.

The server, the researchers say, was left connected to the Internet and did not require a password to allow access to the data within.

Thus, it [exposed more than one million records](#) representing the personally identifiable information (PII) of 30,000 to 40,000 students, the researchers estimate.

The exposed information, they say, included full names, email addresses, and phone numbers, along with credit card information, transaction and purchased meals details, and login information stored in plain text.

SafetyDetectives, which notes that the improperly secured server was being updated at the time it was discovered, also found evidence of server logs showing student data being exposed.

The researchers say that the 5GB database appeared to contain the details of students who are Transact Campus account holders. Given that Transact Campus works with higher education institutions in the United States, the majority of impacted students are US individuals.

Transact Campus provides an application that students can use with a unique personal account (called Campus ID) to make payments and purchases, and which can also be used for activities such as event access, class attendance monitoring, and more.

What the researchers could not determine was whether malicious actors accessed the unprotected database before it was secured.

However, they note that, if bad actors did download the data, the impacted students could fall victim to various types of attacks, including phishing, spam marketing, and scams. Furthermore, since login credentials were stored unencrypted on the server, account takeover attacks are also possible.

SafetyDetectives says they contacted Transact Campus about the unprotected server in December 2021, but did not receive a reply until January 2022, after they had contacted US-CERT as well. The database had already been secured at that time, but Transact Campus denied being responsible for the breach.

“Apparently this was set up by a third party for a demo and was never taken down. We did confirm that the dataset was filled with a fake data set and not using any production data,” Transact Campus told SafetyDetectives.

The researchers, however, told SecurityWeek that they checked a sample of the data found on the server and that they believe it belongs to real people.

“We use publicly available tools to perform random searches for the people exposed and see if they actually exist. We, of course, performed this process when we discovered this server and found out that the data seemed to belong to real people,” SafetyDetectives said.

Contacted by *SecurityWeek*, Transact Campus said they launched an investigation into the breach immediately after being informed of the exposure.

According to Chief Information Security Officer Brian Blakley, the exposed database was found to belong to a third-party and that none of Transact’s servers was accessed without authorization.

When asked whether the potentially impacted students had been warned in any way of the data exposure, Blakley directed *SecurityWeek* to contact Sodexo, which appears to have been responsible for the breach.

“Sodexo in conjunction with its payment’s provider for dining services, Foundry, provided a Notice of Data Breach to impacted clients and users explaining the incident,” he said.

Sodexo provides catering, facility management, and home and personal services across the globe. *SecurityWeek* contacted the company for additional details on the breach, but has yet to receive a response.

**Related:** [Over 300,000 Internet-Exposed Databases Identified in 2021](#)

**Related:** [Over 380,000 Kubernetes API Servers Exposed to Internet: Shadowserver](#)

**Related:** [Cybercriminals Hold 1,200 Unsecured Elasticsearch Databases for Ransom](#)

Share

Tweet

推荐 13



Ionut Arghire is an international correspondent for SecurityWeek.  
Previous Columns by Ionut Arghire: