Turnitin investigates cyberattack on customer-facing systems



Turnitin disclosed unauthorized activity in certain customer-facing systems and says services are operational. It has not said whether data was accessed or how many customers are affected.

- Turnitin, a subsidiary of Advance Publications, reported unauthorized activity involving certain customer-facing systems in a letter dated November 23.
- The company activated its incident response plan, notified the relevant authorities and engaged external cyber experts.
- It says the affected systems do not collect government identification credentials or institutional financial information.
- The company did not say which systems were breached, whether data was accessed, or how many customers are affected.

> - The University of Colorado Boulder reported no indication of exposure and added monitoring of its Canvas integration.

Turnitin, the plagiarism-checking provider used by thousands of education and research institutions worldwide, has disclosed a cyberattack involving certain customer-facing systems. The company is a subsidiary of Advance Publications.

What the company has said

In a letter published on its website on November 23, CEO Chris Caren said Turnitin had identified unauthorized activity. The company started its incident response plan, notified the relevant authorities and opened an investigation with external cyber experts. It states that its systems are fully operational and safe to use, and that the affected customer-facing systems do not collect government identification credentials or institutional financial information. Monitoring continues while the investigation into the nature and scope of the incident goes on.

Customer-facing Turnitin systems include the student submission portal, the instructor grading interface, integration APIs for institutions and reporting dashboards. The company did not say whether any of these were breached, or which ones.

What remains unknown

The company has not said whether any data was accessed or how many customers may be affected. The University of Colorado Boulder said it is in contact with Turnitin to establish whether its information was compromised. It currently has no indication that student or instructor information or assignments were exposed. Because Turnitin is mainly accessed through a Canvas integration, the university added monitoring to confirm Canvas was not affected.

Why it matters for institutions

Education and research bodies that rely on Turnitin, directly or through a learning platform, should treat this as a third-party incident still developing. The facts are limited, and no impact on any particular institution has been confirmed. A measured approach is to seek clarity from the vendor and watch the integration points.

What to do now

1. Confirm whether your institution uses Turnitin directly or through an LMS integration, and identify the business owner.
2. Ask Turnitin in writing whether your tenant or data was affected, and request updates as the investigation proceeds.
3. Add monitoring on LMS and API integrations with Turnitin and review logs for unusual activity.

4. Review which data types are shared with the service and confirm they match your data-classification and PDPL obligations.
5. Check your third-party incident clauses and notification duties, and prepare a short internal brief for leadership.