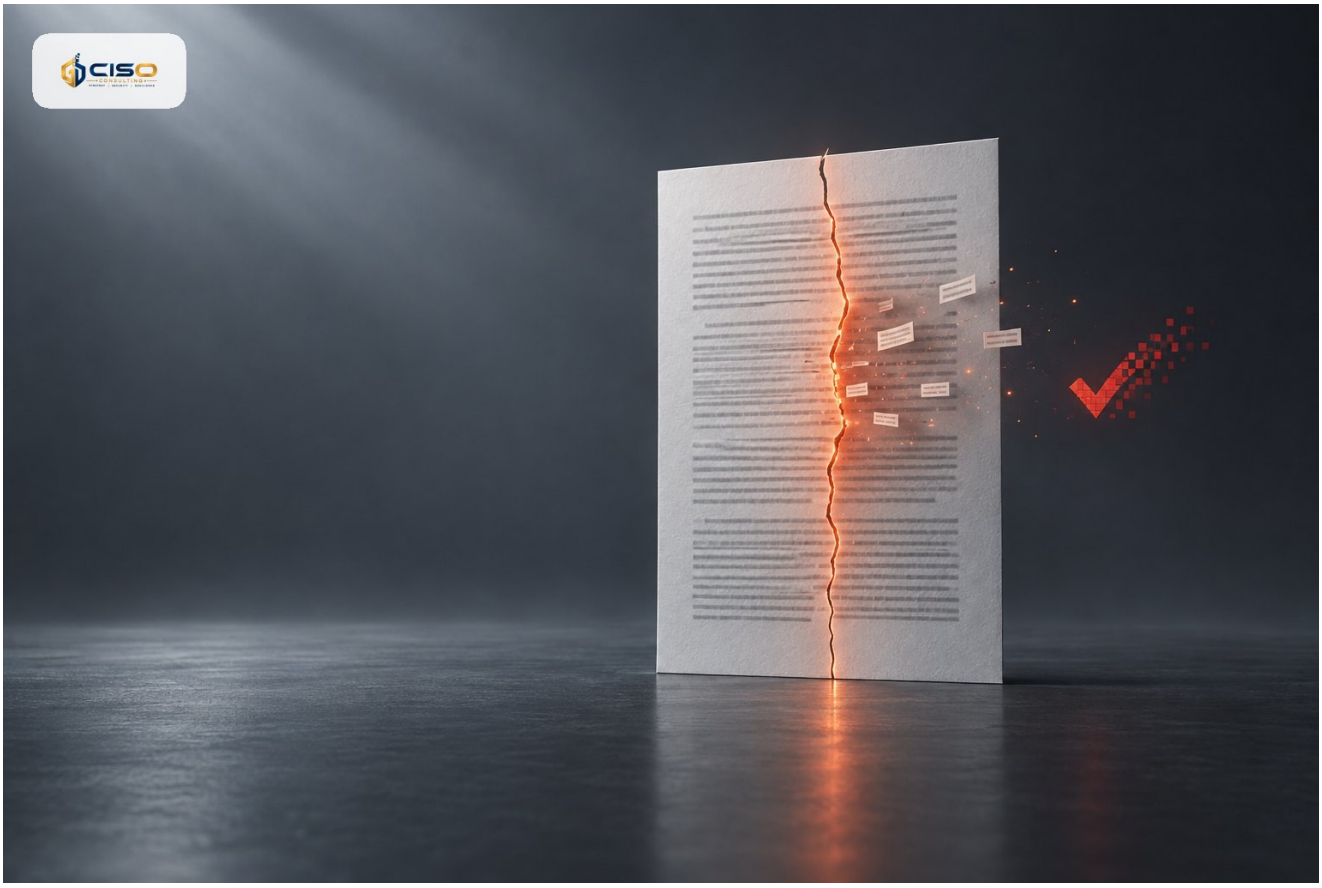
Turnitin discloses unauthorized activity in customer-facing systems



Turnitin says it detected unauthorized activity in some customer-facing systems and activated its incident response plan. The investigation is ongoing, and the company has not said whether user data was accessed.

- Turnitin detected unauthorized activity involving certain customer-facing systems and activated its incident response plan.
- External cybersecurity specialists are assisting; law enforcement and cyber regulators have been notified.
- The company says its systems are fully operational and that the affected systems do not collect government ID credentials or institutional financial information.
- It has not disclosed when the incident occurred, whether user data was accessed, or how many

> people are affected.
> - No ransomware group has publicly claimed responsibility.

Educational technology provider Turnitin has disclosed that it identified unauthorized activity involving certain customer-facing systems. In a public letter, CEO Chris Caren said the company put its incident response plan into action, started an investigation with external cybersecurity specialists, and notified law enforcement and cyber regulators.

What is known

Turnitin states that its systems are fully operational and safe to use, and that the affected systems do not collect government identification credentials or institutional financial information. Its status page shows no incidents for November 2026. The company says it continues to monitor for further unauthorized activity, and its investigation is still under way.

According to the company's website, its software is used by over 16,000 institutions in 185 countries and serves 71 million students. It is known for AI-generated writing detection, digital grading, research integrity checks and exam proctoring.

What is not known

Turnitin has not said when the incident happened, what the unauthorized activity involved, whether any user data was accessed or stolen, or how many people may be affected. No ransomware group has publicly claimed the attack. The company told BleepingComputer it had no further details to share.

Implications for customers

Because the scope is undisclosed, institutions that use the platform cannot yet judge their exposure from public information. A measured approach is to confirm with the vendor what applies to your tenant and to review what data your staff and students upload, while waiting for the investigation to conclude.

What to do now

1. Contact Turnitin through your account channel and ask whether your tenant or data is affected, and request updates as the investigation proceeds.
2. Inventory what data your institution uploads to the platform, including any personal data, and classify its sensitivity.
3. Check whether your contract requires the vendor to notify you of incidents and within what timeframe.
4. If personal data may be involved, assess PDPL notification obligations with your data-protection officer so you are ready if the vendor confirms exposure.

5. Remind staff to watch for phishing that references the platform, and record the vendor in your third-party risk register as an open incident.