Abrigo restores Sageworks after outage linked to irregular activity



Abrigo has restored its Sageworks risk management application, except borrower-facing features, after an outage caused by what it called irregular activity in its environment. The incident is reported as a suspected cyberattack.

- Abrigo is the financial technology company behind the Sageworks risk management application.
- The platform went offline after the company detected irregular activity in its environment.
- The application has been restored, but borrower-facing capabilities remain unavailable.
- The incident is described as a suspected cyberattack; the available source text gives no further detail.

Financial technology company Abrigo has restored its Sageworks risk management application, with the

exception of borrower-facing capabilities. The restoration follows an outage that the company attributed to "irregular activity" in its environment, and the event has been reported as a suspected cyberattack.

What is known

The available information is limited. The platform was taken offline, the core application has since been brought back, and the features that borrowers use directly are still not available. The source excerpt does not say what the activity was, whether data was affected, or when the remaining features will return.

Why it matters for regulated institutions

Sageworks is a risk management application used in lending and credit workflows. An outage at a third-party platform of this kind can interrupt internal processes and customer-facing services at the institutions that depend on it. Institutions that use this or similar providers should treat the event as a prompt to check their own exposure rather than as a confirmed breach of their data.

Suggested approach

Avoid assumptions until the provider shares verified details. Confirm whether your institution uses the service, ask the vendor for formal incident communication, and review how your own continuity and third-party risk arrangements would respond if a critical provider were unavailable for an extended period.

What to do now

1. Check whether any business unit uses Sageworks or other Abrigo services, including through subsidiaries or partners.
2. Request a formal incident notice from the vendor covering scope, data impact and restoration timeline.
3. Activate manual or alternative procedures for borrower-facing processes that remain unavailable.
4. Review the contract and incident notification terms with critical third-party providers.
5. Test continuity plans for extended outage of a critical SaaS provider, in line with SAMA BCM and NCA ECC third-party requirements.