Colorado's myColorado app taken offline after cyberattack; data of about 150,000 people likely stolen



Colorado's IT office took the myColorado app offline after discovering a breach on November 18. Data tied to nearly 150,000 of its 2.1 million users was likely stolen.

- The breach was discovered on the evening of November 18; the state shut the app down and opened an investigation.
- The app has 2.1 million users, and data tied to nearly 150,000 people was likely stolen.
- Investigators have not said what kinds of data were taken.
- The app stayed offline as of Tuesday afternoon; residents can use agency websites and were told to carry physical IDs when travelling.
- The report notes a wider run of attacks on US state and local bodies, including ransomware.

What happened

Colorado's Governor's Office of Information Technology (OIT) said it discovered on the evening of November 18 that attackers had breached myColorado, the app residents use for digital identification, document storage and access to state services. OIT shut the app down and started an investigation. It was still unavailable on Tuesday afternoon.

The state said the app has 2.1 million users and that the attack likely involved theft of data linked to nearly 150,000 people. Investigators declined to say which data was taken. OIT's executive director said protecting user data is the priority and that systems will return once security is restored.

Impact and wider context

Residents were advised to carry physical IDs when travelling for the Thanksgiving holiday, and can still reach state services through agency websites. The state has previously faced attacks on its Department of Higher Education and ransomware incidents at smaller municipalities.

The report also lists other recent incidents at US public bodies, including a ransomware attack on Queens Public Library in New York, a cyberattack on a county sheriff's office in Mississippi, and an attack that knocked West Virginia's legislature offline.

Why it matters for regulated institutions

The case shows how a single digital identity and services platform can become a point of failure for both data and service continuity. The state's fallback to agency websites and physical IDs is a useful example of planning for the loss of a digital channel. Details of the stolen data remain undisclosed, so conclusions about exposure should wait for further official information.

What to do now

1. Review whether any single digital identity or customer-facing app is a sole channel for critical services, and define a tested fallback channel.
2. Confirm that incident response plans cover shutting down a public app, customer communication and a decision on when to restore it.
3. Check breach-notification procedures against PDPL requirements and engage SDAIA and sector regulators as applicable.
4. Inventory the personal data held in customer apps and document stores, and confirm access controls, logging and encryption.
5. Test business continuity for loss of a digital service in line with SAMA BCM or NCA ECC expectations.