Uber notifies nearly 150,000 drivers of data theft after breach at AI provider Fireworks



Uber is notifying nearly 150,000 drivers that their data was stolen when attackers breached AI infrastructure provider Fireworks in early October. The incident is a reminder of third-party exposure.

- Uber is notifying nearly 150,000 drivers about a data breach.
- The attackers stole driver data after breaching Fireworks, an AI infrastructure provider.
- The breach of Fireworks took place in early October.
- The exposure originated at a supplier rather than within Uber's own systems, as described in the source excerpt.

What was reported

Uber has begun notifying nearly 150,000 drivers that their data was stolen. According to the report, the attackers breached Fireworks, a provider of AI infrastructure, in early October, and the driver data was taken as a result.

The source excerpt does not detail which data fields were affected, how the attackers gained access, or what remediation steps have been taken. Those points should not be assumed until fuller information is available.

Why it matters for regulated institutions

The case shows how personal data can be exposed through a supplier that sits behind a well-known brand. Organisations increasingly use external AI platforms and infrastructure, and any personal data shared with them extends the institution's risk perimeter and its accountability for that data.

For institutions in the Kingdom, this touches third-party risk management, data-sharing governance and breach notification readiness, all areas where regulators expect clear ownership and evidence.

Recommended approach

There is no need for alarm, but this is a good moment to confirm what personal and confidential data your AI and other infrastructure suppliers actually hold, and whether your contracts and incident procedures would let you act quickly if one of them were compromised.

What to do now

1. Inventory suppliers, especially AI and cloud platforms, that process your personal or confidential data, and record what data each holds.
2. Review contracts for breach notification timelines, security obligations and audit rights.
3. Minimise the data shared with AI providers, using masking or anonymisation where feasible.
4. Include supplier compromise scenarios in incident response plans and test them.
5. Confirm your PDPL breach assessment and notification process is documented and assigned to owners.