US lawmakers press ID verification firms on data handling after IDScan breach



US lawmakers wrote to identity verification firms after the IDScan breach exposed scans of over 150 million ID documents. They asked how sensitive data is stored and protected. The case is a prompt to review third-party ID data practices.

- A September breach of IDScan's cloud platform led to scans of more than 150 million ID documents appearing for sale on the dark web.
- Six lawmakers asked several identity verification firms to explain how they manage and protect customers' sensitive data.
- They urged proactive vulnerability hunting, zero-trust architecture and minimal collection, sharing and storage of personal data.
- Journalist Brian Krebs reports that more than two dozen such firms store scanned IDs, often by

default, and that customers may pay extra to avoid it.

- Krebs reports that data theft began over a year before the stolen data was found online.

A bipartisan group of six US lawmakers has written to several identity verification companies about their security practices, following a September breach at IDScan. Customer data held in the company's cloud platform was stolen, and scans of more than 150 million drivers' licenses and other identification documents were later offered for sale on the dark web. The FBI is investigating.

What the lawmakers asked

The letter asks the companies for detailed answers on how they handle sensitive customer data and how they defend it against attacks increasingly enabled by artificial intelligence. It urges them to hunt for vulnerabilities proactively, deploy zero-trust architecture, and limit the collection, sharing and storage of personally identifying information as far as possible.

The letter to IDScan's chief executive notes that, besides the ID documents, nearly 600,000 medical cards, employment authorizations and other sensitive records were exposed. The license scans reportedly included ultraviolet and infrared images.

Why it matters beyond the US

Journalist Brian Krebs, who first reported the breach, says he has found more than two dozen identity verification firms that store scanned IDs, often by default, and that customers can have to pay more to stop the scans being retained. He also reports that criminals on the Nexus marketplace began taking the data more than a year before it was discovered online.

The source does not mention any Saudi impact. The lesson is general: organizations that outsource identity verification inherit the risk of whatever the provider keeps, and the retention of ID images is a design choice that can be negotiated and verified.

What to do now

1. Inventory third-party providers that collect or store ID scans or similar identity documents on your behalf.
2. Ask each provider in writing whether scans are retained after verification, for how long, and how to disable retention.
3. Include data minimization, retention limits and deletion evidence in vendor contracts, in line with PDPL obligations.
4. Review vendor security assurance, including cloud access controls, vulnerability management and zero-trust practices.
5. Update incident response plans to cover a vendor-side breach of customer identity data, including

notification steps.