State Bank of India Confirms Customer Data Leak Found on the Dark Web



State Bank of India says 3,897 customer records with personal data were among about 375,000 records on the dark web. The bank has not yet established where the data originated.

- 3,897 customer records with personal information were identified in a set of about 375,000 records on the dark web.
- The bank does not yet know the source of the data.
- The disclosure came in a stock-exchange filing dated October 21.
- The filing described an incident involving the loss of certain data.
- SBI is the largest bank in India and is state-owned.

What was disclosed

State Bank of India, the country's largest bank and a state-owned institution, has confirmed that customer data has surfaced on the dark web. In a stock-exchange filing dated October 21, it said it had experienced an incident involving the loss of certain data.

The bank identified 3,897 customer records containing personal information within a larger set of about 375,000 records available on the dark web.

What is still unknown

According to the report, the bank does not yet know where the data came from. The source does not say how the records were obtained, what fields they contain beyond personal information, or whether the other records in the set relate to the bank.

Until the origin is established, it is difficult to say whether this is a breach of the bank's own systems, of a third party, or a compilation of older data. That uncertainty is itself a useful lesson for other institutions.

Why it matters for Saudi institutions

The case shows that exposure can be discovered externally, before the root cause is understood. Regulated institutions in the Kingdom should be ready to assess and report such an event while the investigation is still open, and to know which customer data sits with which processors and partners.

It is a reasonable moment to test dark-web monitoring, data-inventory accuracy and the decision path for notifying regulators and affected individuals.

What to do now

1. Check that dark-web and leak monitoring covers your brand, customer-data samples and key third parties.
2. Confirm your data inventory shows where customer personal data is held, including with processors and vendors.
3. Rehearse a scenario where leaked data appears with an unknown origin, including triage and attribution steps.
4. Review the PDPL breach-notification path and the timelines for informing the regulator and affected customers.
5. Verify that sector reporting duties to SAMA and NCA are mapped to your incident response plan.