# Third-party provider breach exposes Chase customer data



J.P. Morgan Chase has warned of a data breach after a cyberattack on a third-party service provider exposed customers' personal information and marketing data. The headline also names Visa and Mastercard customers.

- Chase disclosed a data breach originating at a third-party service provider.
- Exposed data includes customers' personal information and marketing data.
- The source headline links the incident to Visa and Mastercard customer information as well.
- The incident is a reminder that vendor security directly affects the institution's own data risk.

## What was reported

J.P. Morgan Chase has warned that it suffered a data breach. According to the report, the cause was a cyberattack on a third-party service provider rather than on the bank's own systems. The exposed information includes customers' personal information and marketing data.

The report's headline also refers to Visa and Mastercard customer information. The excerpt available to us does not give further detail, so the number of people affected, the specific data fields, the provider's identity and the timeline should be confirmed against the full report and official notices.

## Why it matters for Saudi institutions

The incident illustrates a familiar pattern: a bank can hold strong internal controls and still see customer data exposed through a supplier that processes it on its behalf. Marketing and personal data shared with vendors are often less tightly governed than core banking data, yet they can carry the same privacy obligations.

For institutions regulated by SAMA and the NCA, and subject to the PDPL, third-party processors fall within the scope of accountability. That makes vendor inventories, contractual security requirements and incident notification terms practical matters rather than paperwork.

## Recommended approach

No action is needed in response to a specific technical indicator, since none was reported. The sensible step is to use this event to test your own supplier arrangements, starting with vendors that hold customer personal or marketing data.

## What to do now

1. Update the inventory of third-party providers that process customer personal or marketing data.
2. Review contracts for security requirements and clear incident-notification deadlines.
3. Confirm what customer data each vendor holds and remove data they no longer need.
4. Check that your incident response plan covers a breach originating at a supplier, including PDPL notification steps.
5. Request recent assurance evidence from high-risk vendors, such as audit reports or test results.