ROOT CAUSE ANALYSIS

Peach Payments – Paysafe downtime

April 28, 2022

At a glance…

• What was affected?

Ability to access the Paysafe UI was denied during this incident. Main processing platforms remained fully operational and unaffected as did the Paysafe API. Ongoing RCA of symptoms indicate that this is a recurrence of an incident which took place last year.

• What was the root cause?

A major contributor to the issue was identified as being code used for notification of Payment links being generated on PaySafe combined with a lack of appropriate indices on the associated database instance. Once indices were applied to mitigate the poor performance of the code, normalisation of resources on the server began immediately.

• What preventative actions are being taken?

The application is under code freeze with the exception being for security updates as required. The applied indices have been included in the application source for future deployments (if they occur).
Monitoring and notifications have been updated to include early-warning identifiers.

Incident Number	2022042801
Customers Affected	Customers accessing the Paysafe UI
Start Time	April 28, 2022 08:16:00 AM
End Time	April 28, 2022 11:34:00 AM
Impact Duration	minutes

If you have any questions concerning the content of this RCA, please open a case via support@peachpayments.com

Alternatively, please contact your relevant Account Managers for alternative methods of contacting emergency support.

This root cause analysis (RCA) document is a follow-up to the incident detailed above, which resulted in an interruption to Peach Payments Paysafe services. All primary processing platforms remained operational and were unaffected by this event. Additional details are outlined in the following sections.

Resolution Activities

At 10.01 AM SAST merchant escalations identified an incident whereby Paysafe Web UI was failing to render. Application and infrastructure teams joined in war-room to investigate the cause.

Once missing indices were identified, they were applied and latency on the API calls to generate Payment Links began to drop immediately.

Services were restarted and fully restored at 11:34 AM SAST.

Full Root Cause Details

There were a combination of things which together caused this incident; missing indices on the database instance, slow downstream response times for SMTP systems accepting Payment Links emails, a large enough volume of Payment Links being generated and poor design in the code responsible for generating Payment Links.

When a downstream SMTP provider is slow, this generates a long tail of backlogged messages in the database and causes DB queries to become slow to the point of rendering the application unusable. Indexes which were absent from the database were critical to preventing the latency of queries on the specific tables included in a large run of "payment links" being generated via the API. The volume of Payment Links being generated triggers a threshold of latency which results in a runaway exhaustion of DB resources, leading to the query latency and subsequently the long-tail.

Planned Preventative Action Items

Target Date	Action
April 29, 2022	DevOps team has implemented early-warning monitoring on the DB instance to identify the latency threshold in queries which could potentially lead to a similar event.
May 02, 2022	“Code Freeze” declared on the system with the exception of critical security updates as required.