ROOT CAUSE ANALYSIS

Peach Payments – Paysafe UI Outage

May 3rd 2022

At a glance…

- **What was affected?**

The Paysafe UI was unavailable, presenting an HTTP session timeout error to the user

- **What was the root cause?**

Latency in the connection between the DB and the API handling mail delivery causing the DB connections to become stale and generate resource exhaustion on the application server.

- **What preventative actions are being taken?**

Additional performance related indices have been added to the DB, as well as lowering of monitoring and alerting thresholds.

Incident Number	IN2022050301
Customers Affected	Customers using Paysafe UI
Start Time	May 3, 2022 09:57:00 AM
End Time	May 3, 2022 10:19:00 AM
Impact Duration	22 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 services. All primary processing platforms remained operational and were unaffected by this event. Additional details are outlined in the sections below.

Resolution Activities

At 09:53 on May 3rd 2022 our monitoring systems alerted us to high average latency on some queries affecting the Paysafe DB. This latency appeared to be linked to a sudden increase in load on the Paysafe API and while our engineers were investigating the warning notification the Paysafe UI became unreachable.

The symptoms of the outage appeared similar to the outage of April 28th 2022, but were caused by a different set of high-latency queries.

A full and complete audit of the database systems indices was completed and additional performance related indices identified and applied.

At 10:19 services were restored to normal in the Paysafe system.

Full Root Cause Details

A long-running/high-latency query triggered by activity in the application caused resource contention in the available HTTP worker threads capable of processing inbound requests, leading to the site being unavailable.

Planned Preventative Action Items

Target Date	Action
May 3rd	Reduce the Warning and Critical thresholds for specific monitors on the system to increase “early-warning” lead time without triggering false-positive notifications.
May 4th	Perform an audit of all performance related indices on the database and cross-reference them with poorly-performing application queries to identify potential high-latency calls. Apply indices as needed.
May 5th	Document these changes and back-port them to Testing and QA environments.