

## COMPLIANCE EVIDENCE REPORT

# Incident Response and Service Readiness Evidence

This report presents evidence of the incident detection, response and recovery activities of Kestrel Pay Ltd., and of the readiness of its in-scope services, for the reporting period. Evidence is mapped to the AICPA Trust Services Criteria (SOC 2) and to ISO/IEC 27001:2022 Annex A.

|                   |                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------|
| Organization      | Kestrel Pay Ltd. (fictional)                                                              |
| Reporting period  | July 1, 2026 to September 30, 2026                                                        |
| Scope             | 27 production services owned by the payments, platform and database teams                 |
| Frameworks        | SOC 2 (AICPA Trust Services Criteria) · ISO/IEC 27001:2022                                |
| Incident response | SOC 2 CC7.3, CC7.4, CC7.5                                                                 |
| Service readiness | SOC 2 CC1.3, CC7.2, CC8.1, A1.3 · ISO 27001 A.5.9, A.5.26, A.5.30, A.8.15, A.8.16, A.8.32 |
| Generated         | October 1, 2026, 09:00 UTC, by NOFire AI                                                  |
| Report ID         | EVR-2026Q3-7F3AC21                                                                        |

**3 / 3****Incident response criteria supported by complete evidence.**

No exceptions. One observation (section 3.4).

**25 / 27****Services meet all assessed controls.**

Two exceptions (section 6).

# 1. Summary of results

All figures are derived from system records of alerts, pages, acknowledgements, escalations and handoffs captured by NOFire AI during the reporting period. No figures were entered manually.

|                                          |                               |                                             |                                         |
|------------------------------------------|-------------------------------|---------------------------------------------|-----------------------------------------|
| <b>412</b><br>alerts received and routed | <b>38</b><br>incidents opened | <b>4m 12s</b><br>median time to acknowledge | <b>100%</b><br>of on-call hours covered |
|------------------------------------------|-------------------------------|---------------------------------------------|-----------------------------------------|

## 1.1 Incident response criteria

| CRITERION | EVIDENCE SUMMARY                                                                                | POPULATION   | EXCEPTIONS | RESULT      |
|-----------|-------------------------------------------------------------------------------------------------|--------------|------------|-------------|
| CC7.3     | Every alert was evaluated and routed to the team that owns the affected service.                | 412 alerts   | 0          | ✓ Supported |
| CC7.4     | Every incident was paged, acknowledged and escalated according to its team's escalation policy. | 38 incidents | 0          | ✓ Supported |
| CC7.5     | Every incident was resolved, and closed with a handoff note describing the recovery.            | 38 incidents | 0          | ✓ Supported |

## 1.2 Incidents by team

| TEAM     | INCIDENTS | SEV1 | SEV2 | SEV3 | MEDIAN ACK | MEDIAN RESOLVE | ESCALATED |
|----------|-----------|------|------|------|------------|----------------|-----------|
| payments | 17        | 1    | 5    | 11   | 3m 48s     | 41m            | 3         |
| platform | 14        | 0    | 4    | 10   | 4m 30s     | 36m            | 2         |
| database | 7         | 1    | 2    | 4    | 4m 55s     | 58m            | 1         |
| Total    | 38        | 2    | 11   | 25   | 4m 12s     | 42m            | 6         |

## 2. On-call coverage

| SCHEDULE         | ROTATION                 | MEMBERS | HOURS COVERED | OVERRIDES | ESCALATION POLICY                       |
|------------------|--------------------------|---------|---------------|-----------|-----------------------------------------|
| payments-primary | Weekly, Mon 09:00 CET    | 6       | 2,208 / 2,208 | 4         | Primary → secondary at 5m → lead at 15m |
| platform-primary | Weekly, Mon 09:00 CET    | 5       | 2,208 / 2,208 | 3         | Primary → secondary at 5m → lead at 15m |
| database-primary | Two weeks, Mon 09:00 CET | 4       | 2,208 / 2,208 | 2         | Primary → lead at 10m                   |

### 3. Evidence by criterion

#### 3.1 CC7.3 · Evaluation of security events

✓ Supported

The entity evaluates security events to determine whether they could or have resulted in a failure to meet its objectives, and if so, takes action to prevent or address such failures.

**Population:** all alerts received in the period (412). Each alert was associated with the affected service and routed to the owning team under the routing rules in effect. No alert was routed to a fallback or left unassigned. **Exceptions:** none.

412

alerts received

412

routed to an owning team

5

monitoring sources

#### 3.2 CC7.4 · Incident response

✓ Supported

The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate and communicate security incidents.

**Population:** all incidents opened in the period (38). Each incident paged the on-call responder on the owning team's schedule. Six incidents were escalated in accordance with the applicable escalation policy. All acknowledgements and escalations are time-stamped and attributed to named individuals. **Exceptions:** none.

38 / 38

paged per schedule

38 / 38

acknowledged

6 / 6

escalated per policy

#### 3.3 CC7.5 · Recovery from incidents

✓ Supported

The entity identifies, develops and implements activities to recover from identified security incidents.

**Population:** all incidents opened in the period (38). Each incident was resolved by a named responder and closed with a handoff note documenting recovery actions and follow-up items. Post-incident reviews are linked for both SEV1 incidents (INC-4743, INC-4809). **Exceptions:** none.

38 / 38

resolved

38 / 38

closed with a handoff note

2 / 2

SEV1 reviews linked

**3.4 Observation.** On August 14, 2026, a schedule override on payments-primary left a 40-minute gap in coverage (02:00 to 02:40 CET). The secondary responder covered the gap before any alert was received, and coverage for the period remained 100%. This is recorded as an observation, not an exception.

## 4. Incident register

Ten of 38 incidents are shown. The complete register, including all pages and acknowledgements, is provided in Appendix A (incidents-q3-2026.csv).

| INCIDENT | OPENED        | SERVICE       | SEV | ACK    | RESOLVED | ACKNOWLEDGED BY | HANDOFF |
|----------|---------------|---------------|-----|--------|----------|-----------------|---------|
| INC-4821 | Sep 28, 14:02 | payments-api  | 2   | 2m 29s | 29m      | Sam Okafor      | ✓ Yes   |
| INC-4817 | Sep 26, 03:41 | ledger-writer | 3   | 4m 02s | 51m      | Jonas Weber     | ✓ Yes   |
| INC-4809 | Sep 21, 11:18 | pg-main       | 1   | 1m 47s | 1h 34m   | Lena Park       | ✓ Yes   |
| INC-4802 | Sep 17, 22:09 | ingress-gw    | 3   | 5m 10s | 22m      | Ravi Shah       | ✓ Yes   |
| INC-4790 | Sep 9, 07:55  | fraud-scorer  | 2   | 6m 31s | 47m      | Jonas Weber     | ✓ Yes   |
| INC-4774 | Aug 30, 16:20 | checkout-web  | 3   | 3m 12s | 18m      | Sam Okafor      | ✓ Yes   |
| INC-4761 | Aug 22, 02:13 | k8s-prod-eu   | 2   | 4m 44s | 1h 02m   | Ravi Shah       | ✓ Yes   |
| INC-4743 | Aug 14, 19:37 | payments-api  | 1   | 2m 05s | 2h 11m   | Sam Okafor      | ✓ Yes   |
| INC-4728 | Aug 3, 10:51  | pg-replica-2  | 3   | 4m 58s | 39m      | Lena Park       | ✓ Yes   |
| INC-4712 | Jul 19, 13:26 | notify-svc    | 3   | 3m 33s | 15m      | Maya Cohen      | ✓ Yes   |

### 4.1 Timeline: INC-4821

|          |                                                 |
|----------|-------------------------------------------------|
| 14:01:58 | Alert from Datadog: payments-api 5xx above 2%   |
| 14:02:00 | Routed to payments (owner of payments-api)      |
| 14:02:11 | Paged Sam Okafor by push                        |
| 14:04:40 | Acknowledged by Sam Okafor                      |
| 14:19:02 | Escalated to secondary, Jonas Weber, on request |
| 14:31:05 | Resolved by Sam Okafor, handoff note added      |

### 4.2 Handoff note: INC-4821

Rolled back payments-api to v2.41.3 after 5xx rose on the new connection pool settings. Error rate back under 0.1% at 14:27. Follow-up: PAY-2318, load-test pool settings before the next release.

### 4.3 Record integrity

Records are append-only. Corrections are recorded as new entries and do not overwrite prior entries. SHA-256 checksum of Appendix A:

9c1f4e27a3b8d06f5e12c7a94b3d8e60f1a25c97d4b8e3f02a6c19d5e7b84f31

## 5. Service readiness assessment

Each in-scope service was assessed against the controls listed in section 5.2. Assessments are derived from the Kubernetes clusters, cloud accounts and source repositories connected to NOFire AI, and are not self-reported. Each check records its evidence source, whether the result was observed or inferred, and the time of assessment.

Services in scope: **27** · Meeting all assessed controls: **25** · Exceptions: **2** · Assessed: October 1, 2026, 09:00 UTC

### 5.1 Results by service

| SERVICE       | TEAM     | OWNER | ALERTS | SLO | RUNBOOK | CHANGE REVIEW | SOC 2         | ISO 27001     |
|---------------|----------|-------|--------|-----|---------|---------------|---------------|---------------|
| payments-api  | payments | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| ledger-writer | payments | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| fraud-scorer  | none     | ✗     | ✓      | ✓   | ✓       | ✓             | Not compliant | Not compliant |
| checkout-web  | payments | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| rates-cache   | platform | ✓     | ✗      | ✗   | ✓       | ✓             | Not compliant | Not compliant |
| auth-svc      | platform | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| ingress-gw    | platform | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| notify-svc    | platform | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| kafka-events  | platform | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| pg-main       | database | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| pg-replica-2  | database | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |
| k8s-prod-eu   | platform | ✓     | ✓      | ✓   | ✓       | ✓             | Compliant     | Compliant     |

Twelve of 27 services are shown, including both exceptions. The complete list is provided in Appendix B (services-q3-2026.csv).

### 5.2 Controls assessed

| CHECK                  | SOC 2 | ISO 27001      | EVIDENCE SOURCE                                 |
|------------------------|-------|----------------|-------------------------------------------------|
| Owner                  | CC1.3 | A.5.9          | Observed: service catalog and CODEOWNERS        |
| Alerts and SLO         | CC7.2 | A.8.15, A.8.16 | Observed: alert rules and metrics in monitoring |
| On-call and escalation | CC7.4 | A.5.26         | Observed: on-call schedules and policies        |
| Runbook                | A1.3  | A.5.30         | Observed: runbook linked to the service         |
| Change review          | CC8.1 | A.8.32         | Observed: branch protection and approvals       |

## 6. Exceptions

### 6.1 fraud-scorer

SOC 2 Not compliantISO 27001 Not compliant

Tier 2

Customer facing

Calls payments-api, rates-cache

| REQUIREMENT            | CONTROLS                         | STATUS                                    |
|------------------------|----------------------------------|-------------------------------------------|
| Asset ownership        | SOC 2 CC1.3 · ISO A.5.9          | <span>Owner missing</span>                |
| Change management      | SOC 2 CC8.1 · ISO A.8.32         | ✓ <span>Changes reviewed</span>           |
| Monitoring and logging | SOC 2 CC7.2 · ISO A.8.15, A.8.16 | ✓ <span>Alerts and logs in place</span>   |
| Incident response      | SOC 2 CC7.4 · ISO A.5.26         | ✓ <span>On-call and escalation set</span> |
| Recovery               | SOC 2 A1.3 · ISO A.5.30          | ✓ <span>Runbook linked</span>             |

#### FINDING

**Asset ownership not defined.** No owning team has been recorded for fraud-scorer in the service catalog or in CODEOWNERS since September 29, 2026, following the merger of the risk team into payments. Accountability for changes and incidents affecting the service is therefore unassigned. No alerts were received for the service after this date.

**Recommended remediation:** assign an owning team. SOC 2 CC1.3 and ISO 27001 A.5.9 are expected to pass at the next assessment.

### 6.2 rates-cache

SOC 2 Not compliantISO 27001 Not compliant

Tier 2

Internal

Called by fraud-scorer, checkout-web

#### FINDING

**Monitoring not configured.** rates-cache exports metrics, but no alert rule or service level objective is defined for the service (SOC 2 CC7.2; ISO 27001 A.8.16). A failure of rates-cache would affect checkout-web without generating a page.

**Recommended remediation:** define an error-rate alert and an availability SLO. SOC 2 CC7.2 and ISO 27001 A.8.16 are expected to pass at the next assessment.

### 6.3 Changes affecting services with exceptions

| CHANGE   | MERGED | REACHES      | PRE-MERGE FINDING AND OUTCOME                                                                           |
|----------|--------|--------------|---------------------------------------------------------------------------------------------------------|
| PAY-2331 | Sep 30 | fraud-scorer | Change affects a service with no owner. Approved by payments after review.                              |
| PLAT-918 | Sep 24 | rates-cache  | Change reaches checkout-web through a service without alerting. Remediation tracked in PLAT-921 (open). |