INC0010115 — [TITAN] Critical — data_leak on openai-banking-copilot

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	Closed
Resource	openai-banking-copilot	Group	security_engineering
Resource type	Microsoft.CognitiveServices/accounts	Change type	Emergency
Opened	2026-04-22 18:49:22	Closed	2026-04-22 19:03:22
CAB required	Yes	Close code	Successful

Security Finding

```
Banking-copilot OpenAI endpoint received 38 prompts containing raw customer SSNs, account numbers, and card PANs in the last 24h. GLBA §501(b) + PCI DSS 3.4 + SOX ITGC violation — card data + PII leaked into third-party LLM prompt logs. AI GUARD blocked exfiltration and rotated prompts.
```

Justification

```
Critical: Banking-copilot OpenAI endpoint received 38 prompts containing raw customer SSNs, account numbers, and card PANs in the last 24h. GLBA §501(b) + PCI DSS 3.4 + SOX ITGC violation — card data + PII leaked into third-party LLM prompt logs. AI GUARD blocked exfiltration and rotated prompts.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az cognitiveservices account network-rule add --name openai-banking-copilot --resource-group rg-banking-ai --ip-address 10.0.0.0/8 && titan-ai-guard apply-policy --policy banking-strict-pii
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT — finding must no longer appear.
5. Close ticket with Successful close_code.
```

Risk & Impact Analysis

```
Risk level: HIGH business risk — active exposure; fix required immediately.
Business impact if unremediated: Potential data exfil, privilege escalation, or compliance breach.
Scope: single resource (openai-banking-copilot).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Banking-copilot OpenAI endpoint received 38 prompts containing raw customer SSNs, account numbers, and card PANs in the last 24h. GLBA §501(b) + PCI DSS 3.4 + SOX ITGC violation — card data + PII leak
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of openai-banking-copilot before change (baseline: titan-banking-demo-20260422T201922Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
a. TITAN FORGE fires rollback automatically using stored snapshot.
b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.
```

Test Plan

```
1. TITAN SCOUT rescans openai-banking-copilot immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.
```

Recommended Fix Command

```
az cognitiveservices account network-rule add --name openai-banking-copilot --resource-group rg-banking-ai --ip-address 10.0.0.0/8 && titan-ai-guard apply-policy --policy banking-strict-pii
```

Compliance Mapping

```
SOC 2 CC7.1, HIPAA §164.312(b)
```

AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the critical data_leak incident, FORGE applied the consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared, and CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30 days for rollback.
```