CHG0030111 — [TITAN] High — encryption on s3-banking-wire-instructions

Severity	High	Priority	2 - High
Cloud	AWS	State	Assigned
Resource	s3-banking-wire-instructions	Group	security_engineering
Resource type	AWS::S3::Bucket	Change type	Normal
Opened	2026-04-22 19:13:22	Closed	2026-04-22 19:13:22
CAB required	Yes	Close code	—

Security Finding

```
Wire-instruction S3 bucket has server-side encryption disabled — wire fraud staging ground. SWIFT CSP 1.2, PCI DSS 3.4, and Fed Reserve Operating Circular violation.
```

Justification

```
High: Wire-instruction S3 bucket has server-side encryption disabled — wire fraud staging ground. SWIFT CSP 1.2, PCI DSS 3.4, and Fed Reserve Operating Circular violation.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws s3api put-bucket-encryption --bucket s3-banking-wire-instructions
--server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgo
rithm":"aws:kms","KMSMasterKeyID":"alias/banking-wires"}}]}'
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: MEDIUM-HIGH risk — misconfiguration with realistic exploit path.
Business impact if unremediated: Increases attack surface; auditor finding likely.
Scope: single resource (s3-banking-wire-instructions).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: Wire-instruction S3 bucket has server-side encryption disabled — wire fraud
staging ground. SWIFT CSP 1.2, PCI DSS 3.4, and Fed Reserve Operating Circular violation.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of s3-banking-wire-instructions 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 s3-banking-wire-instructions 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

```
aws s3api put-bucket-encryption --bucket s3-banking-wire-instructions
--server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgo
rithm":"aws:kms","KMSMasterKeyID":"alias/banking-wires"}}]}'
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1
```

AI Close Notes

```
TITAN CONDUIT opened this high encryption change request and assigned it to the banking_compliance
group for review. STATE: ASSIGNED — awaiting human action. Per TITAN AI policy (and Kazmi rule,
2026-04-22), configuration changes are NEVER auto-applied and change tickets are NEVER auto-closed
by TITAN. The assigned group reviews the recommended fix, schedules a CAB-approved change window,
applies the fix manually, validates via SCOUT rescan, and closes this ticket themselves. TITAN
documents and routes — the human owns the change from here.
```