# INC0010103 — [TITAN] Critical — fraud on iam-user-fraud-svc-legacy

| | | | |
|---|---|---|---|
| Severity | Critical | Priority | 1 - Critical |
| Cloud | AWS | State | Closed |
| Resource | iam-user-fraud-svc-legacy | Group | banking_compliance |
| Resource type | AWS::IAM::User | Change type | Emergency |
| Opened | 2026-04-22 20:01:22 | Closed | 2026-04-22 20:15:22 |
| CAB required | Yes | Close code | Successful |

## Security Finding

```
Fraud-detection service account has admin access + no MFA + access keys unrotated 420 days. Bank regulator FFIEC CAT mandates least-privilege and MFA on privileged accounts.
```

## Justification

```
Critical: Fraud-detection service account has admin access + no MFA + access keys unrotated 420 days. Bank regulator FFIEC CAT mandates least-privilege and MFA on privileged accounts.
```

## Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws iam attach-user-policy --user-name iam-user-fraud-svc-legacy --policy-arn
arn:aws:iam::aws:policy/FraudOpsReadOnly && aws iam update-access-key --status Inactive
--access-key-id AKIA...
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 (iam-user-fraud-svc-legacy).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: Fraud-detection service account has admin access + no MFA + access keys unrotated
420 days. Bank regulator FFIEC CAT mandates least-privilege and MFA on privileged accounts.
```

## Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of iam-user-fraud-svc-legacy 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 iam-user-fraud-svc-legacy 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 iam attach-user-policy --user-name iam-user-fraud-svc-legacy --policy-arn
arn:aws:iam::aws:policy/FraudOpsReadOnly && aws iam update-access-key --status Inactive
--access-key-id AKIA...
```

## Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, PCI DSS 3.5
```

## AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the critical fraud 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.
```