Case Study: Bank Reconciliation Discrepancy & Potential Data Breach



Background

A professional accounting firm uses cloud-based accounting software with individual staff IDs for traceability. Reconciliations and transaction postings are expected to be staff-driven, ensuring accountability and auditability.

Scenario

During a monthly reconciliation review:

- A bank reconciliation was shown as **completed under a staff member's ID**.
- However, a transaction included in that reconciliation was **not recorded manually by the staff**.
- The **client identified** the discrepancy and raised concerns.
- Investigation revealed that the transaction had been **auto-posted by the system**, but still reflected under the staff's login credentials.

Key Issues

1. **Misattributed Entry** – The auto-posted transaction was incorrectly tagged to the staff ID.
2. **Lack of Transparency** – Neither the staff nor management were aware of the auto-entry until flagged by the client.
3. **Data Integrity Risk** – Auto-generated entries without clear logs suggest possible **system malfunction** or **unauthorised data breach**.
4. **Client Escalation** – Trust concerns arose as the error was caught externally, not internally.

Carisma Solutions confidential. Please do not distribute.

Root Cause Analysis

- **System Issue**: Auto-posting of transactions not linked to user action.
- **Audit Trail Gaps**: Lack of clarity in system logs on auto entries vs. manual entries.
- **Access Security**: Potential misuse of staff ID credentials cannot be ruled out.
- **Process Weakness**: Reconciliation marked as “completed” without validating completeness of transaction recording.

Impact

- **Financial Reporting**: Risk of misstated balances due to unrecorded or misattributed transactions.
- **Operational Efficiency**: Additional investigation time spent, delaying reporting deadlines.
- **Data Security**: Raised suspicion of unauthorised access or system vulnerability.
- **Reputation**: Client confidence shaken due to error detection from their side.

Corrective Actions

- Conduct an **immediate audit** of system logs to trace source of auto entry.
- Engage the **software provider’s support team** to confirm whether auto-posting is a feature, bug, or breach.
- Mandate **dual-review checks** before finalising bank reconciliations.
- Reset and **strengthen staff credentials** (multi-factor authentication).

Carisma Solutions confidential. Please do not distribute.

Preventive Measures

- Enable **system alerts** for auto-posted or system-generated entries.
- Introduce **clear tagging** in the software to differentiate staff vs. system entries.
- Implement a **monthly IT audit** to monitor for irregular login activity.
- Train staff and clients on **escalation protocols** when anomalies are found.
- Regularly **update accounting software** to patch security vulnerabilities.

Outcome (Hypothetical Resolution)

After implementing corrective and preventive measures:

- Auto-entry logs were clarified, reducing misattributed transactions.
- Staff accountability was restored through stronger audit trails.
- Client confidence improved due to transparent handling of the issue.
- Firm initiated an **ongoing cybersecurity review** to prevent recurrence.

Carisma Solutions confidential. Please do not distribute.