INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-04 06:09 UTC

Lloyds Banking Group Mobile App Glitch Exposes Transaction Data of ~447,000 Customers

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0079
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Lloyds Banking Group mobile application (Lloyds, Halifax, Bank of Scotland brands); specific app version(s) not publicly disclosed
Published	2026-04-02
Discovery Source	Gemini

Executive Summary

A software defect in Lloyds Banking Group's shared mobile banking platform exposed transaction histories and personal financial data for approximately 447,000 customers across the Lloyds, Halifax, and Bank of Scotland brands. The root cause appears to be an authorization or session-isolation failure in the app backend, allowing authenticated users to view other customers' transaction data without any credential theft or external attack. No unauthorized fund transfers were reported, but the scale and sensitivity of exposed data triggers UK GDPR notification obligations and FCA reporting requirements, and the UK Treasury Select Committee has characterized the incident as an alarming breach of data confidentiality.

Technical Analysis

The incident stems from a broken access control defect in Lloyds Banking Group's shared mobile banking backend, mapped to CWE-284 (Improper Access Control), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), and CWE-639 (Authorization Bypass Through User-Controlled Key). The failure allowed authenticated sessions to retrieve transaction records belonging to other account holders, consistent with an insecure direct object reference (IDOR) pattern or a session-isolation breakdown in the multi-tenant backend. MITRE ATT&CK technique T1530 (Data from Cloud Storage) is applicable given the cloud-hosted mobile backend architecture typical in modern banking platforms. No CVE has been assigned; this is a software defect, not a publicly disclosed vulnerability. Specific affected app versions have not been disclosed by Lloyds. No exploit code or external threat actor involvement has been identified. The attack vector is internal to the

application layer; no network-level IOCs are associated. Patch or remediation status has not been publicly confirmed by Lloyds as of available reporting.

Action Checklist

1. Containment: If you operate shared mobile backend platforms (multi-brand or multi-tenant), immediately audit session-isolation controls to confirm session tokens cannot retrieve records outside their bound account scope. For Lloyds customers: change your banking app password and monitor account activity for unauthorized transactions. Monitor official Lloyds and FCA communications for remediation confirmation and patch availability.
2. Detection, Review application access logs for anomalous cross-account data retrievals: authenticated sessions returning records where the account identifier in the response does not match the account identifier bound to the session token. Flag any API responses where customer record IDs in returned data differ from the requesting session's bound identity. For organizations assessing their own apps, focus on API gateway logs and backend authorization middleware logs for IDOR-pattern anomalies.
3. Eradication, For organizations operating their own mobile banking or multi-tenant financial platforms, audit all API endpoints that return customer financial records. Enforce server-side authorization checks on every data retrieval call, confirming that the requested object ID maps to the authenticated session's account before returning data. Do not rely solely on client-side or token-presence checks. Reference OWASP API Security Top 10: API1:2023 Broken Object Level Authorization for remediation guidance.
4. Recovery, After applying authorization fixes, validate remediation by testing authenticated sessions against object IDs outside their scope and confirming access is denied with appropriate error codes. Monitor application logs for continued cross-account retrieval attempts post-fix. Confirm with your data protection officer whether a personal data breach notification to the ICO (or relevant authority) is required under UK GDPR Article 33, given the 72-hour reporting window.
5. Post-Incident, This incident exposes a control gap in authorization architecture review for multi-brand, shared-backend platforms. Add IDOR testing and session-isolation validation to your mobile application penetration testing scope. Review your SDLC for mandatory access control verification at the API layer before production deployment. Map findings to NIST SP 800-53 AC-3 (Access Enforcement) and AC-4 (Information Flow Enforcement) to assess control adequacy.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO, DPO, and legal counsel if log analysis confirms that cross-account transaction data was retrieved by any session — even without evidence of intentional exploitation — as this constitutes a personal data breach under UK GDPR Article 4(12) triggering mandatory ICO notification within 72 hours under Article 33, and potentially FCA notification obligations under SYSC 15A.

Recovery Notes	After the server-side object-level authorization fix is deployed, run a full IDOR regression test suite against all transaction-retrieval and account-detail API endpoints before restoring unrestricted customer access to the mobile app. Monitor API gateway logs continuously for a minimum of 30 days post-fix, alerting on any HTTP 200 response to a transaction-retrieval endpoint where the requested account ID does not match the session-bound account ID. Given the 447,000-customer exposure scope and the shared Lloyds/Halifax/Bank of Scotland backend architecture, verify that the fix is confirmed effective independently for each brand's customer segment before declaring the incident closed.
Forensic Artifacts	API gateway access logs: HTTP GET requests to transaction-retrieval endpoints (e.g., /accounts/{accountId}/transactions, /statements, /history) during the glitch window, with session token values, requested account IDs, response HTTP status codes, and response payload sizes — the primary artifact for determining which sessions accessed which accounts. | Session token introspection / identity provider logs: records mapping each session token to its legitimately bound account ID (the 'sub' or 'account_id' claim), used as the ground truth to identify every instance where a token returned data for an account it was not bound to. | Backend application server logs (e.g., Spring Boot, Node.js, or equivalent framework logs for the shared Lloyds/Halifax/Bank of Scotland platform): SQL query logs or ORM query logs showing SELECT statements against the customer transaction table, specifically queries where the WHERE account_id parameter did not match the session-bound account ID. | API response payload samples (if captured by WAF, proxy, or logging middleware): actual response bodies from the cross-account retrieval window, preserved to establish the exact categories of personal financial data exposed (transaction amounts, payee names, dates, account numbers) for UK GDPR Article 33 breach notification content requirements. | Session lifecycle logs from the mobile app backend authentication service: token issuance timestamps, session creation events, and any session state changes during the glitch window — used to reconstruct whether the IDOR was triggered by a specific race condition, shared session cache misconfiguration, or systematic authorization bypass affecting all sessions.

Per-Action IR Details

Containment — Financial institutions and organizations running shared mobile backend platforms should audit their session-isolation controls immediately. If your platform uses a shared backend serving multiple brands or customer segments, verify that session tokens cannot be used to retrieve records outside the authenticated account scope. Lloyds has not published a vendor advisory or patch identifier; monitor official Lloyds, FCA, and ICO communications for remediation confirmation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate the affected capability to prevent continued unauthorized data exposure while preserving evidence of the session-isolation failure scope.

Controls: NIST IR-4 (Incident Handling), NIST AC-3 (Access Enforcement), NIST SC-23 (Session Authenticity), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 6.1 (Establish an Access Granting Process)

Compensating: Without an enterprise API gateway or WAF, a 2-person team can extract API backend logs manually and run a one-time query grouping responses by session token, then diff the account ID bound to each token against all account IDs returned in that session's responses: `grep -E 'accountId|customerId|userId' api-access.log | awk '{print $session_token_field, $returned_account_id_field}' | sort | uniq` — any row where the returned account ID does not match the session-bound ID is a candidate IDOR hit. If the platform is self-operated, temporarily disable or rate-limit API endpoints returning transaction history until server-side object-level authorization can be verified.

Evidence: Before making any configuration changes to the mobile banking backend, preserve: (1) API gateway access logs covering the full window of the glitch — capture raw request logs including session token values, endpoint paths (e.g., /api/v1/accounts/{accountId}/transactions), HTTP response codes, and response payload sizes; (2)

Backend authorization middleware logs showing which object IDs were resolved for each incoming session token; (3) Database query logs (if enabled) showing SELECT statements against the customer transaction table — look for queries where the WHERE clause account ID does not match the session's bound account ID; (4) Session token issuance and binding records from the identity/auth service to establish the ground truth of which token was legitimately bound to which customer account.

Detection — Review application access logs for anomalous cross-account data retrievals: authenticated sessions returning records where the account identifier in the response does not match the account identifier bound to the session token. Flag any API responses where customer record IDs in returned data differ from the requesting session's bound identity. For organizations assessing their own apps, focus on API gateway logs and backend authorization middleware logs for IDOR-pattern anomalies.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate API response payloads against session-bound identity records to identify the full population of cross-account exposures and determine incident scope.

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, parse API gateway access logs using Python or jq: for JSON-structured logs, run `jq 'select(.response.body.accountId != .session.boundAccountId)' api-gateway.log` to surface IDOR hits directly. For text-format logs, use a two-pass approach — first extract session-token-to-account-ID bindings from auth service logs into a lookup table (CSV), then join against API response logs on session token and flag rows where returned account IDs are not in the legitimate set for that token. A free Sigma rule targeting IDOR patterns in API logs (filtering on HTTP 200 responses to /accounts/{id}/transactions where id does not match session claims) can be run against log files using `sigma convert` with a grep or jq backend.

Evidence: Forensic evidence specific to this IDOR/session-isolation failure: (1) API gateway access logs — specifically HTTP GET requests to transaction-retrieval endpoints (e.g., /accounts/{accountId}/transactions, /history, /statements) with HTTP 200 response codes, cross-referenced against session token identity claims; (2) OAuth or session token introspection logs from the identity provider — extract the 'sub' or 'account_id' claim embedded in each token and compare against the account IDs present in API responses served under that token; (3) Response payload size anomalies — a session unexpectedly receiving another customer's full transaction history will produce a response payload size consistent with that customer's transaction volume, which may differ significantly from the authenticated user's expected payload size; (4) Backend application server logs (e.g., Tomcat access logs, Spring Boot request logs) for the shared Lloyds/Halifax/Bank of Scotland backend, filtering on the glitch window timeframe for all /transactions or /accounts endpoint hits.

Eradication — For organizations operating their own mobile banking or multi-tenant financial platforms, audit all API endpoints that return customer financial records. Enforce server-side authorization checks on every data retrieval call, confirming that the requested object ID maps to the authenticated session's account before returning data. Do not rely solely on client-side or token-presence checks. Reference OWASP API Security Top 10: API1:2023 Broken Object Level Authorization for remediation guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the root-cause authorization defect from all API endpoints serving customer financial data, and verify no residual IDOR-vulnerable code paths remain before restoring normal service.

Controls: NIST SI-2 (Flaw Remediation), NIST AC-3 (Access Enforcement), NIST SI-10 (Information Input Validation), NIST SA-11 (Developer Testing and Evaluation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: A 2-person team without enterprise DAST tooling can perform targeted IDOR validation using OWASP ZAP (free) with a custom scan policy: authenticate two separate test accounts against the mobile banking API, capture the transaction-retrieval endpoint URL for Account A, then replay that request substituting Account B's account ID while using Account A's session token — a vulnerable endpoint returns HTTP 200 with Account B's data; a remediated endpoint returns HTTP 403 or HTTP 404. Automate this across all transaction and account-detail

endpoints using ZAP's script console with a Python script iterating over a list of endpoint patterns. Additionally, run a static code review of the authorization middleware layer targeting any function that constructs a database query using a request-supplied account ID parameter without first asserting `session.accountId == request.accountId`.

Evidence: Before deploying the authorization fix, capture: (1) A complete enumeration of all API endpoints in the shared Lloyds/Halifax/Bank of Scotland backend that accept an account ID as a path or query parameter and return financial records — this serves as the authoritative scope of the remediation effort; (2) The specific authorization middleware code path (stack trace or code snippet if accessible) that failed to enforce object-level ownership checks, preserved as a code artifact for the post-incident review; (3) A pre-fix baseline of HTTP response codes and payload hashes for cross-account IDOR test cases, to serve as the comparison baseline for post-fix validation testing.

Recovery — After applying authorization fixes, validate remediation by testing authenticated sessions against object IDs outside their scope and confirming access is denied with appropriate error codes. Monitor application logs for continued cross-account retrieval attempts post-fix. Confirm with your data protection officer whether a personal data breach notification to the ICO (or relevant authority) is required under UK GDPR Article 33, given the 72-hour reporting window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore service only after authorization controls are verified, and sustain heightened monitoring of transaction-retrieval API endpoints to detect any residual or attempted cross-account access.

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST SI-6 (Security And Privacy Function Verification), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Post-fix validation without enterprise tooling: run a structured IDOR regression test using curl or Postman — authenticate as Customer A, capture the session token, then issue `curl -H 'Authorization: Bearer ' https://api.bankingplatform.example/accounts//transactions` and assert the response is HTTP 403 with no financial data in the body. Repeat for every endpoint pattern identified during eradication. For ongoing monitoring, configure an API gateway access log alert (or a daily cron job parsing logs with grep/awk) that fires on any HTTP 200 response to a transaction-retrieval endpoint where the path account ID does not match the session-bound account ID — this is the same detection query from the Detection phase, now serving as a regression monitor.

Evidence: Before closing out recovery, preserve: (1) Post-fix IDOR test results — documented HTTP 403/404 responses with timestamps for every cross-account test case, confirming the authorization fix is effective across all endpoint variants; (2) API access logs from the first 24-72 hours post-fix, retained to demonstrate to the ICO and FCA that cross-account data retrieval ceased after remediation was applied; (3) A timestamped record of when the fix was deployed to production, the specific code change or configuration applied, and the results of post-deployment validation testing — this constitutes the breach remediation evidence package for regulatory notification purposes under UK GDPR Article 33.

Post-Incident — This incident exposes a control gap in authorization architecture review for multi-brand, shared-backend platforms. Add IDOR testing and session-isolation validation to your mobile application penetration testing scope. Review your SDLC for mandatory access control verification at the API layer before production deployment. Map findings to NIST SP 800-53 AC-3 (Access Enforcement) and AC-4 (Information Flow Enforcement) to assess control adequacy.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct a lessons-learned review focused on why server-side object-level authorization was absent or ineffective in the shared Lloyds/Halifax/Bank of Scotland backend, and update SDLC gates, pen test scope, and architecture review checklists to prevent recurrence in multi-brand shared platforms.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), NIST SA-11 (Developer Testing and Evaluation), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: A 2-person team can implement SDLC guardrails at low cost using: (1) a mandatory OWASP ASVS Level 2 checklist item for 'Verify that all API endpoints serving customer financial records enforce server-side object

ownership validation' as a pre-production deployment gate; (2) a custom OWASP ZAP scan policy configured for IDOR detection, integrated into the CI/CD pipeline as a blocking test against the staging environment before any release touching transaction-retrieval APIs; (3) a lightweight architecture decision record (ADR) template requiring documentation of the authorization enforcement point for any new API endpoint that accepts a customer identifier as a parameter — this creates an auditable paper trail for future SDLC reviews without requiring enterprise tooling.

Evidence: Post-incident artifacts to retain for lessons-learned and regulatory purposes: (1) The full incident timeline — from the earliest log evidence of cross-account data exposure through containment, eradication, and recovery completion — including the estimated number of customer records exposed and the duration of exposure; (2) Root cause analysis artifact identifying the specific code path, architectural decision, or configuration that caused session-isolation failure in the shared Lloyds/Halifax/Bank of Scotland backend; (3) Updated SDLC gate documentation and pen test scope addendum showing IDOR and session-isolation testing has been formally added as a required pre-production control for all mobile banking API releases; (4) ICO/FCA breach notification records (if filed), including submission timestamp, notification content, and any regulatory response received.

Detection Guidance

No network-level IOCs are associated with this incident; the exposure was an internal application defect, not an external attack. For organizations assessing their own platforms for similar weaknesses, focus detection on: (1) API gateway logs showing authenticated requests where the object ID in the query or path parameter does not match the account ID bound to the session token; (2) backend application logs showing data retrieval responses that include customer identifiers outside the requesting session's account scope; (3) anomalous volume of distinct account record accesses from a single session token within a short time window, which may indicate opportunistic data harvesting by a user who discovered the defect. For this specific Lloyds incident, there are no published IOC patterns, hashes, or indicators to match against. Affected customers should be notified directly by Lloyds per UK GDPR obligations.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

NIST-800-53R5

- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Lloyds, Bank of Scotland and Halifax apps showed customers ... - BBC	https://www.bbc.com/news/articles/c4g23npxpwgo	T2
Lloyds, Halifax and Bank of Scotland 'technical glitch' showing other ...	https://uk.finance.yahoo.com/news/lloyds-halifax-bank-scotland-tech...	T3
Lloyds admits nearly half a million banking customers affected by ...	https://www.techradar.com/pro/security/lloyds-admits-nearly-half-a-...	T3
Lloyds exposes 447000 customers' data in app glitch - Cybernews	https://cybernews.com/security/lloyds-half-million-customers-data-b...	T3
Lloyds, Bank of Scotland and Halifax customers able to see OTHER ...	https://www.msn.com/en-us/money/personalfinance/lloyds-bank-of-scot...	T3

Generated 2026-04-04 06:09 UTC by TJS Security Command Center