INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-25 06:50 UTC

Citizens Bank customers’ personal information compromised in data breach

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0102
Type	Data Breach
Severity	HIGH
Affected Products	Citizens Bank customers (third-party vendor, vendor identity unconfirmed in available sources)
Published	2 days ago
Discovery Source	Serper

Executive Summary

A third-party vendor serving Citizens Bank exposed the personal information of thousands of bank customers. The vendor's identity, the specific data types compromised, and the breach vector have not been confirmed in available public reporting. The business risk centers on regulatory exposure under financial data protection requirements, customer trust erosion, and potential downstream fraud targeting affected account holders.

Technical Analysis

This incident is classified as a third-party/supply chain exposure event (MITRE ATT&CK T1199, Trusted Relationship) affecting Citizens Bank customers through an unnamed service provider. The associated weakness is CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). No CVE, CVSS score, or technical vulnerability identifier has been published. The specific breach vector, whether misconfiguration, unauthorized access, insider threat, or external intrusion, has not been disclosed. No patch, advisory, or remediation guidance has been issued by Citizens Bank or the unnamed vendor in available sources. Attribution to a threat actor has not been established. Source quality is limited to regional news and payments trade press (Tier 3 only); no official breach notification from Citizens Bank or a regulatory filing has been identified in available reporting. Data types exposed have not been confirmed publicly.

Action Checklist

1. Step 1: Containment, Identify all third-party vendors and service providers with access to Citizens Bank customer data. Determine whether your organization has a vendor relationship with Citizens Bank or uses

overlapping service providers. If a shared vendor is identified, request immediate access revocation pending vendor confirmation of breach scope.

2. Step 2: Detection, Review third-party access logs for anomalous data transfers or API calls originating from vendor-managed integrations in the 90 days preceding this report. Query SIEM for outbound data volume spikes from vendor-connected segments. No specific IOCs or event IDs are available from current public reporting.

3. Step 3: Eradication, No specific patch or remediation has been published. If the breached vendor is identified, revoke API tokens, rotate shared credentials, and terminate active sessions associated with that vendor. Enforce least-privilege access for all vendor integrations while investigation is ongoing.

4. Step 4: Recovery, Validate that vendor access has been scoped to minimum necessary permissions. Confirm customer PII is not accessible via vendor-facing APIs or file shares without explicit authorization. Monitor for anomalous account activity in customer-facing systems post-containment.

5. Step 5: Post-Incident, Audit third-party risk management program for gaps: vendor inventory completeness, contractual breach notification timelines, and data minimization enforcement. Map all vendors with access to customer PII against current risk tiering. This incident highlights T1199 (Trusted Relationship) as an active exploitation pattern against financial institutions, update threat model accordingly.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, compliance, and executive leadership if the breached vendor is confirmed to have accessed or transmitted your organization's customer PII, as this triggers GLBA Safeguards Rule breach notification obligations and potential state-level data breach notification requirements within jurisdiction-specific timeframes (typically 30–72 hours).
Recovery Notes	Post-containment monitoring should focus on customer-facing systems for fraud indicators — specifically new device enrollments, beneficiary additions, address changes, and high-value transfers — for a minimum of 90 days, as threat actors holding breached financial PII typically monetize it through account takeover attempts within that window. Re-validate vendor access permissions weekly for the first 30 days after re-authorization to detect privilege creep. Confirm with the vendor in writing that their own eradication and recovery steps are complete before restoring any integration, and obtain a third-party attestation or SOC 2 Type II update if contractually available.

Forensic Artifacts	API gateway or web server access logs (Apache/Nginx/IIS) covering 90 days pre-disclosure, filtered to vendor source IPs — these will show URI patterns, data volume per request, and frequency anomalies consistent with bulk PII extraction via vendor-trusted API calls exploiting a T1199 Trusted Relationship vector | Active Directory service account audit logs: Event ID 4624 (Logon), 4648 (Explicit Credential Logon), and 4672 (Special Privileges Assigned) for all vendor-associated service accounts, covering the 90-day lookback window to establish access timeline and privilege use | File server or cloud storage object-access logs (Windows Security Event ID 4663 on-prem, or AWS S3 CloudTrail 'GetObject' events) for PII-bearing directories and buckets, filtered to vendor account SIDs or IAM roles — these establish what customer records were read, when, and in what volume | Firewall and NetFlow session logs showing cumulative bytes transferred from PII-hosting segments to vendor egress IP ranges, segmented by day — an exfiltration event against a financial vendor's customer database would appear as a sustained or spiked outbound volume anomaly rather than the low-volume transactional baseline typical of legitimate integrations | Vendor-facing VPN or remote access gateway authentication logs showing session establishment, duration, and data transfer totals for the incident window — these corroborate or contradict the vendor's own breach timeline and scope claims, and are critical for regulatory notification accuracy

Per-Action IR Details

Step 1: Containment — Identify all third-party vendors and service providers with access to Citizens Bank customer data. Determine whether your organization has a vendor relationship with Citizens Bank or uses overlapping service providers. If a shared vendor is identified, request immediate access suspension pending vendor confirmation of breach scope.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CA-3 (Information Exchange), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without a CMDB or vendor management platform, conduct vendor enumeration manually: pull all active service accounts from Active Directory using 'Get-ADUser -Filter {Description -like "*vendor*" -or Description -like "*service*"} | Select Name, Description, LastLogonDate | Export-Csv vendors.csv'. Cross-reference against firewall outbound rules to Citizens Bank IP ranges or shared vendor API endpoints. A two-person team can divide this: one enumerates AD service accounts, the other reviews firewall NAT/outbound rules.

Evidence: Before suspending access, snapshot the current state: export all vendor-associated service account last-logon timestamps and group memberships from Active Directory; capture netstat output on any API gateway or file transfer host to document active vendor sessions ('netstat -anob > active_connections_.txt'); preserve firewall connection logs showing outbound sessions to vendor-managed IP ranges for the 90-day lookback window; pull access control lists on file shares or S3 buckets containing customer PII to establish what the vendor account could have read.

Step 2: Detection — Review third-party access logs for anomalous data transfers or API calls originating from vendor-managed integrations in the 90 days preceding this report. Query SIEM for outbound data volume spikes from vendor-connected segments. No specific IOCs or event IDs are available from current public reporting.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

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

Compensating: Without a SIEM, use PowerShell to parse Windows Security Event Log for large outbound file operations from vendor service accounts: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4663 -and

$_.Message -match ""}'. For API gateways running on Linux, parse access logs with: 'awk \'{print $1, $7, $10}\' /var/log/nginx/access.log | sort -k3 -rn | head -100' to surface the highest-byte-count requests from vendor IP ranges. Use Wireshark with a capture filter on vendor VLAN segments ('host ') to identify exfiltration-sized transfers. Flag any single session transferring more than your established baseline for that integration.

Evidence: Collect and preserve: web application or API gateway access logs (Apache/Nginx /var/log/*/access.log or IIS C:\inetpub\logs\LogFiles\) showing vendor IP source addresses, URI patterns, HTTP response codes, and response body sizes for the 90-day window; Windows Security Event ID 4663 (Object Access — file read) and Event ID 4656 (Handle Requested) on file servers hosting customer PII, filtered to vendor service account SIDs; NetFlow or firewall session logs showing cumulative bytes transferred to vendor egress IPs, segmented by day to identify volume anomalies; any DLP alerts or email gateway logs if customer data was staged and transmitted via email or encrypted archive.

Step 3: Eradication — No specific patch or remediation has been published. If the breached vendor is identified, revoke API tokens, rotate shared credentials, and terminate active sessions associated with that vendor. Enforce least-privilege access for all vendor integrations while investigation is ongoing.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without a PAM platform, use the following manual sequence: (1) Disable vendor AD service accounts immediately — 'Disable-ADAccount -Identity '; (2) Rotate any shared API keys or OAuth client secrets in the vendor integration portal and invalidate existing tokens; (3) On Linux API hosts, revoke active sessions by killing processes owned by the vendor account — 'pkill -u '; (4) Audit and tighten ACLs on PII-holding file shares using 'icacls /remove ' and re-grant only the minimum required paths. Document each action with timestamps for your incident timeline.

Evidence: Before revoking, capture: a full export of the vendor service account's current group memberships, permissions, and last-activity timestamps ('Get-ADUser -Properties * | Export-Csv'); the current ACL state of all PII data stores accessible to the vendor account ('icacls > acl_snapshot_.txt' or 'aws s3api get-bucket-policy --bucket '); any OAuth token issuance logs from your identity provider showing when vendor tokens were last issued and their scope; active session records from your API gateway or VPN concentrator identifying sessions that must be forcibly terminated.

Step 4: Recovery — Validate that vendor access has been scoped to minimum necessary permissions. Confirm customer PII is not accessible via vendor-facing APIs or file shares without explicit authorization. Monitor for anomalous account activity in customer-facing systems post-containment.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 3.3 (Configure Data Access Control Lists), CIS 6.1 (Establish an Access Granting Process)

Compensating: Use osquery to continuously validate that no vendor-associated accounts have regained access to sensitive data paths: 'SELECT username, path, action FROM file_events WHERE username IN ("") AND path LIKE "/data/pii/%"'. For Windows environments, enable object access auditing on PII directories via Group Policy (Audit Object Access — Success/Failure) and monitor Event ID 4663 for vendor SID activity post-containment. Set up a cron job or Task Scheduler entry to run daily permission audits and diff the output against the post-eradication baseline to catch privilege creep.

Evidence: Post-containment, collect and retain: permission audit snapshots of all PII-bearing data stores taken immediately after access revocation, compared against the pre-incident state to document scope of over-permission; API gateway logs confirming zero successful authentication events from revoked vendor tokens after the revocation timestamp; customer-facing application logs (authentication, account inquiry, and transaction logs) from the 30 days post-containment to detect downstream fraud activity by threat actors using compromised customer PII obtained from

the vendor breach; any anomalous login or account-change events in customer banking portal logs (focusing on new device registrations, address changes, and beneficiary additions).

Step 5: Post-Incident — Audit third-party risk management program for gaps: vendor inventory completeness, contractual breach notification timelines, and data minimization enforcement. Map all vendors with access to customer PII against current risk tiering. This incident highlights T1199 (Trusted Relationship) as an active exploitation pattern against financial institutions — update threat model accordingly.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-8 (Incident Response Plan), NIST CA-3 (Information Exchange), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: A two-person team can execute a lightweight third-party risk audit using a spreadsheet-based vendor inventory: column fields should include vendor name, data types shared (PII/PCI/PHI), access method (API/SFTP/VPN), contractual breach notification SLA, last risk review date, and risk tier (critical/high/medium/low). Cross-reference against the AD service account export from Step 1 to identify undocumented vendor accounts. For threat model updates, import the MITRE ATT&CK Navigator layer for T1199 (Trusted Relationship) and map your current detective controls — free at attack.mitre.org/techniques/T1199. Document gaps where no detection exists for vendor-initiated data access.

Evidence: For the lessons-learned record, preserve: the complete vendor access audit trail produced during this incident as the baseline for future third-party risk reviews; contractual agreements with all PII-handling vendors to assess whether breach notification clauses were triggered and met; the incident timeline documenting the gap between breach occurrence (unknown), public disclosure, and your organization's internal detection — this gap measurement feeds directly into your Detection Mean Time to Detect (MTTD) metric for NIST 800-61r3 §4 reporting; regulatory notification assessment documentation under applicable financial sector requirements (GLBA Safeguards Rule, state breach notification laws) that must be retained regardless of whether notification was ultimately required.

Detection Guidance

No IOCs, log signatures, or behavioral indicators have been published in available reporting. Detection approach should focus on third-party access anomalies: review data egress from vendor-connected integrations, audit API gateway logs for unusual query volumes or off-hours access, and check for unauthorized exports from customer data stores. If your organization uses the same unnamed vendor, treat all data shared with that vendor as potentially compromised until vendor clarification is received. Monitor dark web channels and fraud intelligence feeds for Citizens Bank customer data appearing in credential markets.

Framework Mappings

MITRE-ATTACK

- **T1199** — Trusted Relationship

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

NIST-800-53R5

- **SR-2** — Supply Chain Risk Management Plan

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
	https://www.wpri.com/money/citizens-bank-customers-personal-informa...	T3
Citizens Bank customers' personal information compromised in data ...	https://www.yahoo.com/news/articles/citizens-bank-customers-persona...	T3
The personal information of thousands of Citizens Bank customers ...	https://www.facebook.com/WPRI12/posts/the-personal-information-of-t...	T3
Citizens Bank Customers Targeted in Third-Party Data Breach	https://www.pymnts.com/cybersecurity/2026/citizens-bank-customers-t...	T3
Data of Citizen Bank customers compromised in data leak - YouTube	https://www.youtube.com/watch?v=5aBgxCerru8	T3

DISCLAIMER

Generated 2026-04-25 06:50 UTC by TJS Security Command Center