INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:41 UTC

Data Breach Exposes 25 Million Americans in What Texas Calls the Largest US Hack in History

DATA BREACH | CRITICAL

SCC Item ID	SCC-DBR-2026-0037
Type	Data Breach
Severity	CRITICAL
Affected Products	Conduent (US government contractor), client state benefit systems including Texas and New Jersey; specific internal platforms not publicly disclosed as of reporting date
Published	2026-03-05

Executive Summary

A reported breach at Conduent, a government business process outsourcing contractor, allegedly exposed personally identifiable information (PII) for approximately 25 million Americans, including Social Security numbers belonging to state benefit recipients in Texas, New Jersey, and potentially other states, according to Texas officials and media reports. Texas officials have characterized this as the largest government-adjacent contractor breach in US history. Organizations with Conduent contracts or that share data with state benefit systems should treat this as a third-party data exposure event and assess downstream liability, notification obligations, and identity protection commitments to affected individuals.

Technical Analysis

Confirmed breach of Conduent-managed environments supporting state and local government benefit administration. Exposed data includes Social Security numbers and PII for approximately 25 million individuals. No CVE assigned; this is a contractor environment compromise rather than a discrete software vulnerability. CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) applies. MITRE ATT&CK techniques associated with this incident type: T1530 (Data from Cloud Storage), T1078 (Valid Accounts), T1567 (Exfiltration Over Web Service), T1537 (Transfer Data to Cloud Account). Specific attack vector, initial access method, and intrusion timeline have not been publicly disclosed by Conduent or affected states as of the compilation date. No CVSSv3 score is applicable; no CISA KEV entry exists for this incident. Patch or remediation status is not publicly available. Root cause analysis and forensic findings have not been released.

Action Checklist

1. Step 1, Inventory: Identify all active and historical contracts or data-sharing agreements with Conduent. Determine whether your organization's data or your constituents' data was within Conduent-managed systems.
2. Step 2, Third-party notification: Contact your Conduent account representative formally and in writing to request confirmation of whether your data was in scope, obtain a breach notification letter, and request their forensic timeline and root cause summary.
3. Step 3, Regulatory assessment: Engage legal and compliance to evaluate state breach notification obligations (GLBA, state consumer protection statutes, HIPAA if benefits data intersects health information) triggered by third-party exposure of your clients' or constituents' data.
4. Step 4, Vendor risk review: Escalate Conduent's risk rating in your vendor risk management program. Review contractual data protection obligations, right-to-audit clauses, and cyber incident notification SLAs. Suspend non-essential data transfers pending root cause clarity.
5. Step 5, Long-term controls: Require documented evidence of Conduent's post-breach remediation (access control hardening, MFA enforcement, cloud storage policy review). Update third-party risk questionnaires to include cloud data storage segmentation and exfiltration monitoring controls. Validate that future contracts mandate NIST SP 800-53 SC-28 (Protection of Information at Rest) and AC-17 (Remote Access) compliance attestation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership and external IR firm immediately if: (1) Conduent confirms your organization's data was exposed, (2) regulatory filing deadline is <14 days away, or (3) Conduent cannot provide forensic timeline/root cause within 5 business days (indicates possible ongoing compromise or cooperation failure).
Recovery Notes	Post-containment recovery: (1) Once Conduent provides root cause (access mechanism, lateral movement path), conduct a retrospective IR tabletop with your team to validate whether similar access patterns exist in your own estate (use MITRE ATT&CK mapping of Conduent incident to inform your hunt), (2) update your incident response playbook with third-party breach handling procedures and add Conduent to your critical vendor escalation list, (3) schedule quarterly risk reviews of all remaining high-risk vendors and require evidence of continuous MFA and exfiltration monitoring within 90 days.
Forensic Artifacts	Conduent API access logs / authentication logs (request from vendor: user logins, source IPs, API token usage, failed auth attempts) | Your organization's firewall/proxy logs for Conduent IP range (past 180 days: identify data volume anomalies, unusual access times, exfiltration patterns) | Your data warehouse / ETL scheduler logs (job logs showing Conduent data ingestion: frequency, row counts, load duration—compare to baseline for signs of tampering or unusual queries) | Windows Event Log 4688 (Process Creation) / Linux auditd logs from systems accessing Conduent APIs (identify which service accounts/processes initiated data transfers, correlate with Conduent's attacker-controlled account findings) | Email audit logs and DLP alerts (message logs with Conduent in To/From, flagged for external sharing; compare to pre-breach baseline for abnormal communication patterns)

Per-Action IR Details

Step 1 — Inventory: Identify all active and historical contracts or data-sharing agreements with Conduent. Determine whether your organization's data or your constituents' data was within Conduent-managed systems.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation Phase — tools and resources)

Controls: NIST 800-53 SA-9 (External Information System Services), NIST 800-53 SA-4 (Acquisition Process), CIS 6.2 (Third-Party Risk Management)

Compensating: Create a spreadsheet audit: query contract management systems (or manual file review) for Conduent vendor name variations; cross-reference with active data flow diagrams and system interconnection documentation; use grep to search procurement databases and email archives for 'Conduent' + state agency keywords. Validate results against Conduent's public customer list if available.

Evidence: Capture: (1) procurement/contract database exports with metadata timestamps, (2) data flow diagrams showing Conduent system endpoints, (3) email archives mentioning Conduent data transfers, (4) network firewall rules and DNS logs showing Conduent IP ranges/domains (to confirm data pathway scope), (5) active directory group memberships tied to Conduent account provisioning.

Step 2 — Third-party notification: Contact your Conduent account representative formally and in writing to request confirmation of whether your data was in scope, obtain a breach notification letter, and request their forensic timeline and root cause summary.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Analyzing incident data and developing indicators)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 SA-12 (Supply Chain Protection), CIS 6.2 (Third-Party Risk Management)

Compensating: Preserve all communications in a dedicated folder with legal hold applied; document exact timestamp and method of contact (email, certified mail); request Conduent provide: (a) list of systems/tables accessed, (b) data element inventory (PII types, count estimates), (c) breach discovery date and confirmation method, (d) estimated exposure window (access start/end dates). If Conduent delays >72 hours, escalate to legal and file with state regulators as potential notification violation.

Evidence: Capture BEFORE contacting: (1) baseline of your current user/system access logs to Conduent platforms (establish pre-incident state), (2) screenshots of your active data feeds from Conduent systems, (3) network packet captures showing Conduent data ingestion (to compare against attacker exfil IOCs if later disclosed), (4) audit logs from your data warehouse/ETL showing Conduent data load frequency and volume.

Step 3 — Regulatory assessment: Engage legal and compliance to evaluate state breach notification obligations (GLBA, state consumer protection statutes, HIPAA if benefits data intersects health information) triggered by third-party exposure of your clients' or constituents' data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Determining whether an incident response is necessary)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 IR-4 (Incident Handling), CIS 6.2 (Third-Party Risk Management)

Compensating: Create a regulatory decision matrix: (1) map your state(s) of operation to breach notification thresholds (e.g., Texas requires notification if breach affects Texas residents; California's CCPA applies if CA residents' data was exposed), (2) identify affected data types and match to HIPAA/GLBA/state benefit laws, (3) document the chain: your organization → Conduent → affected individuals (establishes your notification obligation), (4) set calendar reminders for state AG notification deadlines (typically 30-60 days from discovery). Archive this mapping as evidence of due diligence.

Evidence: Capture BEFORE legal assessment: (1) your current privacy policy and data processing agreements with Conduent (to identify what you promised constituents), (2) your state benefit/eligibility data retention inventory (to quantify exposure), (3) historical breach notification communications from your organization (for template consistency and precedent), (4) audit logs showing when your team first discovered the Conduent breach (incident discovery

timestamp for statute-of-limitations clock).

Step 4 — Vendor risk review: Escalate Conduent's risk rating in your vendor risk management program. Review contractual data protection obligations, right-to-audit clauses, and cyber incident notification SLAs. Suspend non-essential data transfers pending root cause clarity.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment, Eradication, and Recovery)

Controls: NIST 800-53 SA-9 (External Information System Services), NIST 800-53 CA-8 (Penetration Testing), NIST 800-53 IR-4 (Incident Handling), CIS 6.2 (Third-Party Risk Management)

Compensating: Manually audit your Conduent data feeds: (1) document current data transfer frequency and volume, (2) identify which internal systems depend on Conduent data (map dependencies), (3) redirect non-critical feeds to NULL or sandbox environments immediately via firewall rules or application config changes, (4) for critical feeds, implement compensating controls: dual-source the data (if alternate vendor exists), add checksums/hash validation to detect tampering, log all data ingestion with syslog to a non-Conduent destination. Document all changes with timestamps for forensic record.

Evidence: Capture BEFORE suspension: (1) active data flow snapshots showing current Conduent data volume, frequency, and destination systems, (2) network flow logs (firewall, proxy) for past 90 days showing Conduent communication patterns (baseline for comparison), (3) your vendor risk scoring tool outputs (current ratings, to show escalation magnitude), (4) contract terms document (SLAs, audit rights, incident reporting clauses—for legal review), (5) recent security questionnaires or attestations Conduent provided (to establish baseline security posture at time of agreement).

Step 5 — Long-term controls: Require documented evidence of Conduent's post-breach remediation (access control hardening, MFA enforcement, cloud storage policy review). Update third-party risk questionnaires to include cloud data storage segmentation and exfiltration monitoring controls. Validate that future contracts mandate NIST SP 800-53 SC-28 (Protection of Information at Rest) and AC-17 (Remote Access) compliance attestation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities) and NIST 800-53 CA-7 (Continuous Monitoring)

Controls: NIST 800-53 SA-9 (External Information System Services), NIST 800-53 SC-28 (Protection of Information at Rest), NIST 800-53 AC-17 (Remote Access), NIST 800-53 IA-5 (Authentication and Identification), CIS 6.2 (Third-Party Risk Management)

Compensating: Create a Conduent remediation checklist: request dated attestation letters signed by Conduent CISO/VP stating: (1) MFA deployment scope (% of users, which systems), (2) access review completion date and sample results, (3) cloud storage inventory and encryption status (ask for bucket/container names and ACL screenshots), (4) exfiltration monitoring tool deployed (tool name, rule count, alert samples). For renewal/new contracts, embed compliance requirement as a binding exhibit; tie payment tranches to milestone attestation (e.g., 30% held pending MFA completion proof). Document all attestations in contract file.

Evidence: Capture BEFORE accepting remediation evidence: (1) your current third-party risk questionnaire template (as baseline), (2) Conduent's most recent security assessment report (if any SOC 2, ISO audit, or vendor questionnaire responses exist—dated before breach to show pre-breach posture), (3) your existing contract with Conduent (to identify amendment language needed), (4) industry benchmark contracts from peer organizations (to validate SC-28 and AC-17 inclusion norms). Post-remediation: preserve all dated attestation letters, MFA deployment screenshots, access control policy documents, and cloud storage audits in a dedicated compliance archive with chain-of-custody metadata.

Detection Guidance

Direct detection within your environment is limited unless your organization shares infrastructure or authentication federations with Conduent. Focus detection efforts on the following: (1) Review identity and access logs for any Conduent-associated service accounts, federation tokens, or API credentials that authenticate into your systems, look for anomalous access times, unusual data volume pulls, or access from unexpected source IPs. (2) If your organization uses cloud storage buckets or object stores accessible by Conduent, audit access logs for T1530-consistent behavior: large bulk GET or LIST operations, especially from non-standard user agents or IPs outside contracted access windows. (3) For organizations receiving or processing state benefit data, monitor for unusual outbound data transfers (T1567) from systems that handle that data, flag transfers to non-approved cloud services or file-sharing endpoints. (4) Check for T1078 indicators: review authentication logs for valid-credential logins that deviate from established baselines (off-hours access, new geolocations, privilege escalation following login). (5) No public IOCs (IPs, domains, hashes) have been released by Conduent, CISA, or affected states as of the compilation date. Monitor CISA advisories and the Texas DIR and New Jersey OIT disclosure channels for updated indicators.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1567** — Exfiltration Over Web Service
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

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

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

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
T1078	Valid Accounts	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
	https://www.yahoo.com/news/articles/data-breach-exposes-25-million-...	T3
Data Breach Exposes 25 Million Americans in What Texas Calls the ...	https://www.extremetech.com/internet/data-breach-exposes-25-million...	T3
Conduent data breach exposed 25 million Americans - New York Post	https://nypost.com/2026/02/09/business/conduent-data-breach-exposed...	T3
Americans warned as 'largest breach in US history' robs over 25 ...	https://www.the-sun.com/tech/16002576/conduent-new-jersey-contracto...	T3
Texas Officials Report Largest Data Breach Exposing 25M ...	https://www.linkedin.com/posts/extend-resources_data-breach-exposes...	T3

Generated 2026-03-29 18:41 UTC by TJS Security Command Center