INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:43 UTC

Conduent Data Breach Could Affect 25M People. Learn How to Protect Your Online Accounts

DATA BREACH | CRITICAL

SCC Item ID	SCC-DBR-2026-0012
Type	Data Breach
Severity	CRITICAL
Affected Products	Conduent Incorporated, business process services platform; downstream clients include healthcare payers and government benefit programs
Published	2 weeks ago

Executive Summary

Conduent, a business process outsourcing firm serving major healthcare payers and government benefit programs, suffered a ransomware attack resulting in the exfiltration of personally identifiable information and likely protected health information for at least 25 million individuals. The breach propagated through Conduent's client ecosystem, meaning affected individuals are customers of Conduent's downstream clients rather than Conduent directly. Organizations that contract Conduent for payment processing or back-office services face regulatory exposure under HIPAA and state privacy laws, potential civil liability, and reputational risk from a breach they did not control.

Technical Analysis

Conduent experienced a ransomware intrusion in which threat actors exfiltrated sensitive data prior to encryption, consistent with double-extortion tactics. The incident involves PII and, given Conduent's healthcare payer and government benefits client base, likely PHI as defined under HIPAA. No CVE has been assigned; this is an operational incident, not a software vulnerability disclosure. Relevant CWE mappings reflect the attack surface: CWE-284 (Improper Access Control), CWE-311 (Missing Encryption of Sensitive Data), and CWE-693 (Protection Mechanism Failure). MITRE ATT&CK techniques consistent with this incident pattern include T1078 (Valid Accounts, likely initial access vector), T1566 (Phishing, common precursor), T1190 (Exploit Public-Facing Application), T1486 (Data Encrypted for Impact, ransomware execution), and T1041 (Exfiltration Over C2 Channel). As of the configuration date (2026-03-04), Conduent has not publicly disclosed the full scope of compromised data types, the specific initial access vector confirmed, or patch or remediation status. The Texas Attorney General has opened an investigation. Source quality score for this item is 0.567, reflecting limited primary-source disclosure; technical details above are based on reported incident characteristics and consistent ATT&CK patterns, not confirmed forensic findings.

Action Checklist

1. Step 1, Vendor Inventory: Identify all active and recent contracts with Conduent or Conduent-operated systems; determine which business processes, data types, and individual populations are in scope.
2. Step 2, Data Exposure Assessment: Work with Conduent's breach notification team to obtain a data map of what specific records were exfiltrated; request confirmation of whether your organization's data is included in the 25M affected.
3. Step 3, Regulatory Notification Review: Engage legal and privacy counsel to assess HIPAA breach notification obligations (60-day rule), applicable state breach notification laws, and any government program reporting requirements triggered by PHI or PII exposure.
4. Step 4, Third-Party Risk Posture: Review contractual data security requirements, SLAs, and right-to-audit clauses in your Conduent agreement; initiate a formal incident inquiry under those terms.
5. Step 5, Downstream Monitoring: Enable enhanced monitoring for credential-based attacks and social engineering targeting individuals whose PII may now be in threat actor possession; consider whether affected individuals require notification and credit monitoring support.
6. Step 6, Supply Chain Control Review: Audit third-party access controls for all business process outsourcing vendors; verify that least-privilege, MFA, and data minimization controls are enforced across similar vendor relationships.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	If Conduent's incident response team cannot confirm within 48 hours whether your organization's data is in the exfiltrated set, or if your organization processes PHI for HIPAA-covered entities, escalate to Chief Information Security Officer (CISO), General Counsel, and Chief Privacy Officer immediately to assess notification timeline and regulatory reporting obligations.
Recovery Notes	Post-containment recovery: (1) Conduct mandatory security awareness training for all employees on phishing and social engineering, with emphasis on healthcare/benefits-related pretexts used against Conduent breach victims. (2) Implement MFA on all external vendor access points (VPN, cloud applications, API gateways) if not already enforced; enforce 90-day credential rotation for all service accounts with Conduent or similar BPO vendors. (3) Establish quarterly vendor security reviews with mandatory attestation of incident-free status and control compliance; update your vendor risk assessment policy to require immediate notification of any security events affecting third parties with access to your data.
Forensic Artifacts	Windows Event Log Security (Event ID 4624, 4625, 4720, 4722 for account creation/modification and authentication attempts) | Linux /var/log/auth.log and /var/log/audit/audit.log for SSH authentication and system call auditing | Database transaction logs (SQL Server: fn_dblog, MySQL: binary logs) showing all data exports to Conduent | VPN concentrator logs (Cisco ASA, Fortinet FortiGate, or Palo Alto Panorama) for third-party access patterns and connection sources | Email gateway logs (mail server headers, SMTP transaction logs) for phishing attempts targeting affected individuals | Application-level audit logs from business process systems showing data access, transfers, and user actions related to Conduent integration | Network packet captures (tcpdump/tshark) from data exfiltration period showing communication patterns to Conduent IP ranges

Per-Action IR Details

Step 1, Vendor Inventory: Identify all active and recent contracts with Conduent or Conduent-operated systems; determine which business processes, data types, and individual populations are in scope.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: asset inventory and baseline documentation)

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 SA-9 (External Information System Services), CIS 2.1 (Asset Inventory)

Compensating: Export all vendor contracts from procurement/legal repositories into a single spreadsheet indexed by vendor name, contract ID, data types handled (PII, PHI, financial), and system access scope. Cross-reference against Active Directory groups, VPN access logs, and application user lists to identify actual active connections. Use grep to search email archives and SharePoint for references to Conduent system names and IP ranges: grep -ri 'conduent\|conduent-operated' /mnt/email_archive /mnt/sharepoint_dump.

Evidence: Capture before inventory starts: (1) Current Active Directory group memberships with creation dates to establish active vs. dormant vendor access; (2) VPN access logs (last 90 days) showing connection sources and user identities; (3) Network traffic captures from DMZ/egress points showing data exfiltration baseline to Conduent IP ranges (use tcpdump or tshark on border router); (4) Application audit logs showing data transfers to third-party systems; (5) HR offboarding records to identify contractors no longer active.

Step 2, Data Exposure Assessment: Work with Conduent's breach notification team to obtain a data map of what specific records were exfiltrated; request confirmation of whether your organization's data is included in the 25M affected.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Analysis phase: determine scope and impact); §3.2.5 (Initial notification and escalation)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 AU-2 (Audit Events), CIS 6.2 (Security Event Logging)

Compensating: Without direct access to Conduent's forensic investigation, reconstruct the scope manually: (1) Query your database for all records transferred to Conduent in the attack window (request date range from Conduent's public disclosure); (2) Cross-reference exported record counts against Conduent's reported 25M total to estimate your proportion; (3) Use SQL to identify record types (e.g., SELECT DISTINCT data_type, COUNT(*) FROM conduent_transfers WHERE transfer_date BETWEEN '2024-01-01' AND '2025-01-31' GROUP BY data_type); (4) Request Conduent's incident response contact and formal written confirmation of breach scope within 48 hours under contractual incident notification clauses.

Evidence: Capture before data assessment: (1) Database transaction logs showing all data exports to Conduent, including record counts, timestamps, and user IDs (enable full query logging if not already active); (2) Data retention/backup snapshots from the suspected attack window to quantify what data was accessible; (3) Email communications with Conduent documenting data volumes and types sent in the past 24 months; (4) Any prior breach notifications or security questionnaires completed for Conduent (they often reveal data scope).

Step 3, Regulatory Notification Review: Engage legal and privacy counsel to assess HIPAA breach notification obligations (60-day rule), applicable state breach notification laws, and any government program reporting requirements triggered by PHI or PII exposure.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (Initial notification and escalation)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 SI-4 (Information System Monitoring), CIS 2.7 (Data Protection)

Compensating: Create a regulatory compliance matrix: (1) List all jurisdictions where affected individuals reside (request from Conduent or infer from customer address data); (2) Map state breach notification thresholds (most require notification for any unencrypted PII, some exempt encrypted data—consult state attorney general websites); (3) For HIPAA-covered entities: note the 60-day notification clock starts when the breach is discovered, not

disclosed—document discovery date/time in writing; (4) For government programs (Medicare, SSDI, unemployment): contact program-specific security officers and request incident reporting procedures; (5) Maintain a signed decision log of legal counsel's recommendations with dates to establish due diligence.

Evidence: Capture before regulatory review: (1) Conduent's public breach disclosure statement (screenshot and archive for legal hold); (2) Your organization's privacy impact assessment or data inventory for Conduent-processed data (must exist under HIPAA/HITECH); (3) A signed attestation from your data controller/processor showing when you became aware of the breach (critical for 60-day clock); (4) List of all individuals affected (PII/PHI counts by state or program) to quantify notification scope.

Step 4, Third-Party Risk Posture: Review contractual data security requirements, SLAs, and right-to-audit clauses in your Conduent agreement; initiate a formal incident inquiry under those terms.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment, eradication, and recovery); §3.3.1 (Containment strategy)

Controls: NIST 800-53 SA-3 (System Development Life Cycle), NIST 800-53 SA-9 (External Information System Services), NIST 800-53 CA-8 (Penetration Testing), CIS 4.5 (Third-Party Risk Management)

Compensating: Without legal resources, draft a formal incident inquiry letter (template: use SANS incident response template or CIS supply chain risk guidance): (1) State the date you became aware of the breach; (2) Request Conduent provide within 10 business days: forensic investigation report, timeline of unauthorized access, confirmation of data types/volumes affected, remediation steps, and proof of security control fixes; (3) Cross-reference your contract against NIST 800-53 SA-9(a)(1) baseline requirements (encryption, access controls, incident response procedures) and document gaps; (4) If contract lacks breach notification or audit clauses, escalate to procurement/legal for future vendor management; (5) Document all correspondence in a central incident ticket for regulatory/legal hold purposes.

Evidence: Capture before incident inquiry: (1) Complete executed Conduent contract, including data processing addendum (DPA) or business associate agreement (BAA if HIPAA-covered); (2) Most recent vendor security assessment (SOC 2 Type II report, if available) with audit dates and findings; (3) Previous audit rights exercises or security questionnaire responses to establish baseline vendor compliance; (4) Internal risk assessment or vendor scorecard showing Conduent's prior security rating; (5) Email chains documenting any prior security incidents, complaints, or compliance findings involving Conduent.

Step 5, Downstream Monitoring: Enable enhanced monitoring for credential-based attacks and social engineering targeting individuals whose PII may now be in threat actor possession; consider whether affected individuals require notification and credit monitoring support.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Analysis phase: detect indicators of compromise and related activity)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AC-2 (Account Management), NIST 800-53 AU-12 (Audit Generation), CIS 6.1 (Security Awareness)

Compensating: (1) Enable authentication logging on all systems (Windows Event Log 4624/4625 for login attempts, SSH /var/log/auth.log for Linux): check for impossible travel (logins from Conduent-breach-associated geolocations appearing within minutes of valid user logins), failed MFA attempts in patterns, or new device registrations; (2) Monitor email gateway logs for phishing indicators: emails with subjects containing affected individual names, healthcare terminology, or benefits-related keywords sent to your domain (use grep on mail gateway logs: grep -i 'medicare\|benefits\|health\|account suspended' /var/log/mail*); (3) Alert on credential stuffing patterns: 10+ failed login attempts in 5 minutes from same source IP; (4) Notify affected individuals within your organization's required timeframe (check state breach laws) with recommendation to monitor credit reports and enable fraud alerts with the three bureaus (Equifax, Experian, TransUnion); (5) If budget permits, offer 12-24 months of free credit monitoring through a breach notification vendor.

Evidence: Capture before enabling downstream monitoring: (1) Baseline authentication logs from 30 days prior to know normal login patterns, volumes, and geolocations; (2) List of affected individuals with birthdates and last 4 SSN for cross-reference against credential stuffing attempts; (3) Mail gateway logs from prior 90 days to establish baseline phishing patterns and false positive rate before tuning detection rules; (4) VPN access logs, if applicable, to identify internal user authentication baseline; (5) Screenshot of current monitoring configuration (if any) to establish

pre-incident state.

Step 6, Supply Chain Control Review: Audit third-party access controls for all business process outsourcing vendors; verify that least-privilege, MFA, and data minimization controls are enforced across similar vendor relationships.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3.2 (Eradication phase); NIST 800-61r3 §2.1 (Preparation: baseline and hardening)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 AC-6 (Least Privilege), NIST 800-53 IA-2 (Authentication), NIST 800-53 SA-9 (External Information System Services), CIS 5.3 (Access Control), CIS 5.4 (MFA)

Compensating: (1) Audit all third-party vendor access in Active Directory: query for service accounts older than 12 months without recent password changes (Get-ADUser -Filter 'lastLogonDate -lt $date90DaysAgo' | Export-Csv vendor_stale_accounts.csv); (2) Review VPN and application access logs to enumerate all active vendor connections: parse VPN concentrator logs for source IPs and authenticate user identities against vendor master list; (3) For each BPO vendor, verify: (a) documented least-privilege scope (data types, systems, record volumes allowed); (b) MFA enforcement in authentication logs (check for MFA bypass or passwordless auth without secondary factor); (c) data minimization (query database for actual data volumes transferred vs. contractual limits); (4) Disable or recycle all vendor credentials not actively used in the past 90 days; (5) Implement quarterly attestation from each vendor certifying no data breaches, unauthorized access, or control failures; (6) Create a compensating control matrix documenting which NIST 800-53 controls are enforced at your organization vs. delegated to vendors—identify gaps and assign ownership.

Evidence: Capture before supply chain audit: (1) Current Active Directory schema export showing all service accounts, last password change, and group memberships (ldifde -d 'CN=Users,DC=...' -f ad_export.ldf); (2) VPN access logs from the past 90 days with source IP, destination system, user identity, and connection duration; (3) Application audit logs for data export functions showing which users/service accounts accessed sensitive data and what was transferred; (4) Current vendor contract inventory with MFA, encryption, and incident response requirements documented; (5) Prior security assessments (SOC 2, vulnerability scans) for all BPO vendors to establish baseline control maturity.

Detection Guidance

Direct detection within your environment is limited because the compromise occurred at Conduent's infrastructure, not within customer networks. Focus detection efforts on downstream risk indicators. (1) Credential abuse: Monitor for anomalous authentication activity on accounts associated with individuals or systems that interact with Conduent-processed data; look for impossible travel, off-hours access, or unfamiliar device fingerprints in identity logs (SIEM query: failed + successful auth sequences from new ASNs or geolocations against high-value accounts). (2) Phishing and social engineering: Expect spear-phishing campaigns targeting individuals whose PII was exfiltrated; tune email gateway rules for lure themes related to healthcare benefits, government payments, or breach notification impersonation. (3) Data broker and dark web monitoring: If your organization has threat intelligence subscriptions, task them to monitor paste sites, ransomware leak portals, and dark web marketplaces for Conduent-attributed data sets. (4) Vendor portal access: Review access logs for any Conduent-connected portals or APIs your organization operates; look for unusual query volumes, bulk data pulls, or access from Conduent IP ranges outside of expected windows. No confirmed IOCs have been publicly released as of the configuration date; IOC section reflects this absence.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	Not available	No confirmed IOCs have been publicly disclosed by Conduent or investigative authorities as of 2026-03-04. This field will be updated when verified indicators are released.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling

OWASP-TOP10-2021

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

CIS-V8

- **6.1**

- **6.2**

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)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Cnet	https://www.cnet.com/tech/services-and-software/conduent-data-breac...	T3
Conduent data breach grows, affecting at least 25M people	https://techcrunch.com/2026/02/24/conduent-data-breach-grows-affect...	T2

Source	URL	Tier
Conduent Data Breach Could Affect 25M People. Learn How to ...	https://x.com/CNETNews/status/2027179699873472963	T3
Conduent Data Breach Could Affect 25M People. Learn ... - Reddit	https://www.reddit.com/r/Identity_Protection/comments/1ric87m/condu...	T3
Texas Attorney General Investigates 25M+ Conduent Business ...	https://www.hipaajournal.com/conduent-business-solutions-data-breach/	T3

Generated 2026-03-29 18:43 UTC by TJS Security Command Center