INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 19:24 UTC

Strategic Education Data Breach Exposes SSNs and Government IDs of 100,000+ Individuals

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0149
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Strategic Education, Inc. (operator of Strayer University and Capella University), customer/student data systems
Published	2026-06-04
Discovery Source	Gemini

Executive Summary

Between February 23-25, 2026, Strategic Education, Inc., parent company of Strayer University and Capella University, sustained a data breach exposing Social Security numbers, driver's license numbers, and passport numbers for more than 100,000 individuals across Texas, Massachusetts, and Maine. The attack vector has not been publicly disclosed. The organization faces compounding risk from state regulatory notification obligations and active class action litigation investigation.

Technical Analysis

The breach occurred over a confirmed 48-hour window (February 23-25, 2026) targeting Strategic Education's customer and student data systems. Exposed data classes include government-issued identifiers: Social Security numbers, driver's license numbers, and passport numbers, all high-value for identity fraud and synthetic identity schemes. No CVE has been assigned; this is an incident-based breach, not a disclosed software vulnerability. Applicable CWEs: CWE-284 (Improper Access Control), CWE-693 (Protection Mechanism Failure), CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). Mapped MITRE ATT&CK techniques: T1530 (Data from Cloud Storage), T1078 (Valid Accounts), T1005 (Data from Local System), T1657 (Financial Theft). No threat actor group has been publicly attributed. The initial access method, whether credential compromise, exploitation of an unpatched service, or insider action, remains unconfirmed in public disclosures. Total affected population is undisclosed beyond the 100,000+ records that triggered state notification obligations; actual breach scope may exceed disclosed figures. Public information sourced from litigation tracking and news aggregation sites; no dedicated vendor security advisory has been published.

Action Checklist

1. Step 1: Containment. If your organization has data-sharing, integration, or vendor relationships with Strategic Education, Inc. (Strayer University, Capella University), immediately audit active API connections, SSO integrations, and shared data repositories. Suspend any automated data feeds pending confirmation that the breach perimeter is closed. Reference NIST AC-20 (Use of External Systems), enforce documented terms and conditions for all third-party system access.
2. Step 2: Detection. Review identity and access logs for any accounts shared with or provisioned through Strategic Education systems (T1078, Valid Accounts). Query SIEM for authentication events from Strategic Education IP ranges or domains. Monitor for anomalous outbound data transfers consistent with T1530 (cloud storage exfiltration) and T1005 (local system data collection). Apply CIS 8.2 (Collect Audit Logs), confirm logging is active across all systems that interface with the affected organization. No public IOCs have been released; detection must rely on behavioral patterns rather than signature matching at this time.
3. Step 3: Eradication. No vendor patch or configuration advisory has been published. If credential compromise (T1078) is confirmed as the vector, enforce immediate credential rotation for all shared or federated accounts per NIST AC-7 (Unsuccessful Login Attempts). Enforce MFA on all externally exposed applications per CIS 6.3. Restrict data access to least-privilege roles per NIST AC-6 (Least Privilege). Remove or disable any dormant accounts per CIS 5.3 (Disable Dormant Accounts, 45-day threshold).
4. Step 4: Recovery. Validate that all third-party data connections to Strategic Education systems are documented and access-controlled per NIST AC-20. Confirm audit logging is intact and generating complete records per NIST AU-3 (Content of Audit Records) and AU-12 (Audit Record Generation). Run a privilege access review against NIST AC-6 and AC-2 (Account Management) to confirm no unauthorized accounts remain active. Monitor for downstream identity fraud indicators, particularly synthetic identity use of SSN + government ID combinations, over the next 90 days.
5. Step 5: Post-Incident. This breach exposes gaps in third-party data governance and government identifier handling. Conduct a formal review of data inventory per CIS 3.2 (Establish and Maintain a Data Inventory) to identify where SSNs and government IDs are stored, transmitted, or shared. Assess data access control lists per CIS 3.3. Review external system authorization policies under NIST AC-20. Implement or audit data minimization practices, government identifiers should not be retained beyond operational necessity (NIST AC-23, Data Mining Protection). Prepare regulatory response documentation for any state breach notification obligations applicable to your organization's student or customer population.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if your organization shares SSN, driver's license, or passport number data with Strategic Education, Inc. systems, or if forensic review reveals any outbound data transfers to Strategic Education IP ranges during or after February 23–25, 2026 — these conditions trigger mandatory breach notification obligations under Maine 10 MRSA §1347, Massachusetts 201 CMR 17.00, and Texas HB 4181, and create direct exposure to the active class action litigation investigation.

Recovery Notes	Post-containment, maintain elevated monitoring on all identity and access logs for accounts that had any integration with Strategic Education systems for a minimum of 90 days, as SSN and government ID combinations exposed in this breach are typically weaponized for synthetic identity fraud on a delayed timeline — expect fraud attempts 30–180 days post-breach. Verify that all data-sharing agreements with Strategic Education, Inc. are reviewed and reauthorized under updated terms before any suspended API connections or data feeds are restored, with written confirmation from Strategic Education that the breach perimeter is fully closed and independent forensic review is complete. Preserve all incident artifacts — network logs, access logs, account exports, and timeline documentation — under legal hold given the active class action litigation investigation, ensuring a minimum retention period consistent with applicable state statutes of limitations.
Forensic Artifacts	API gateway and web proxy logs for the February 23–25, 2026 window showing request/response sizes to Strategic Education domains (strayer.edu, capella.edu, strategiceducation.com) — anomalously large response payloads or bulk record-count query patterns would indicate PII extraction via an authorized integration being abused | IdP federation and SSO assertion logs (SAML response logs, OAuth token issuance logs) for all accounts with Strategic Education relying-party trust relationships — these capture whether valid credentials were used to authenticate and pull student or customer PII records during the breach window, consistent with T1078 (Valid Accounts) | Cloud storage access logs (AWS CloudTrail 'GetObject'/'ListBucket', Azure Blob Storage diagnostic logs, Google Workspace Drive Audit) for any shared data repositories containing SSN or government ID fields — bulk read operations on PII datasets during off-hours are the primary T1530 indicator in this breach context | Active Directory and application-layer account audit logs showing privilege assignments, group membership changes, and last-logon timestamps for service accounts used in Strategic Education integrations — these establish whether any account was compromised and used to access PII data beyond its intended scope | Data loss prevention (DLP) or email gateway logs for any outbound transmissions containing regex-matching SSN patterns ('\b\d{3}-\d{2}-\d{4}\b') or passport number formats during February 20–28, 2026 — in the absence of DLP tooling, proxy logs filtered on large POST body sizes to external destinations serve as the compensating artifact

Per-Action IR Details

Step 1: Containment — If your organization has data-sharing, integration, or vendor relationships with Strategic Education, Inc. (Strayer University, Capella University), immediately audit active API connections, SSO integrations, and shared data repositories. Suspend any automated data feeds pending confirmation that the breach perimeter is closed. Reference NIST AC-20 (Use of External Systems) — enforce documented terms and conditions for all third-party system access.

NIST Phase: Containment

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Use 'netstat -anob' (Windows) or 'ss -tunap' (Linux) to enumerate active outbound connections to Strategic Education IP ranges (resolve strayer.edu, capella.edu to IPs first via 'nslookup'). Block identified IP ranges at the perimeter firewall using a temporary deny-all ACL. For SSO integrations (SAML/OAuth), manually disable the identity provider trust relationship in your IdP admin console (e.g., Okta, ADFS) for any Strategic Education-affiliated relying party. Document every suspended feed with timestamp for chain-of-custody.

Evidence: Before suspending feeds, capture: (1) firewall flow logs showing outbound connections to Strategic Education IP ranges and domains (strayer.edu, capella.edu, strategiceducation.com) during February 23–25, 2026 and the 30 days prior; (2) API gateway access logs showing request frequency, payload sizes, and authentication tokens

used for any Strategic Education integrations — anomalously large response payloads may indicate bulk PII extraction; (3) SSO/federation logs from your IdP showing authentication assertions issued to Strategic Education relying parties, including account identifiers and session timestamps.

Step 2: Detection — Review identity and access logs for any accounts shared with or provisioned through Strategic Education systems (T1078 — Valid Accounts). Query SIEM for authentication events from Strategic Education IP ranges or domains. Monitor for anomalous outbound data transfers consistent with T1530 (cloud storage exfiltration) and T1005 (local system data collection). Apply CIS 8.2 (Collect Audit Logs) — confirm logging is active across all systems that interface with the affected organization. No public IOCs have been released; detection must rely on behavioral patterns rather than signature matching at this time.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following: (1) On Windows identity infrastructure, query Security Event Log for Event ID 4624 (successful logon) and 4648 (explicit credential logon) filtering on accounts federated with or provisioned by Strategic Education systems — use 'Get-WinEvent -FilterHashtable @{LogName="Security"; Id=4624} | Where-Object {$_.Message -match "strayer|capella|strategiceducation"}'. (2) For T1530 cloud exfiltration detection, review cloud storage access logs (S3 CloudTrail, Azure Monitor, Google Workspace Admin Audit) for GetObject or download events involving files containing SSN-pattern data ('\b\d{3}-\d{2}-\d{4}\b') during and after February 23–25, 2026. (3) Deploy a Sigma rule against Windows Event Logs filtering on T1005 artifacts: Event ID 4663 (object access) on directories housing student or HR PII data. Free tool: use Chainsaw (GitHub: WithSecureLabs/chainsaw) to parse Event Log files offline with Sigma rules if no SIEM is available.

Evidence: Capture before analysis: (1) Windows Security Event Log entries (Event IDs 4624, 4625, 4648, 4672) for all service accounts and federated identities tied to Strategic Education integrations, covering February 20–28, 2026; (2) DNS query logs from your resolver showing lookups for Strategic Education domains — a spike in lookups or queries from non-standard internal hosts may indicate lateral movement or data staging; (3) Proxy/web gateway logs showing HTTP POST or PUT requests with anomalously large body sizes to external Strategic Education endpoints, which would indicate bulk data being pushed outbound; (4) Cloud storage audit logs (AWS CloudTrail 'GetObject', Azure Blob Storage diagnostic logs) for any buckets or containers holding shared student/customer PII with Strategic Education.

Step 3: Eradication — No vendor patch or configuration advisory has been published. If credential compromise (T1078) is confirmed as the vector, enforce immediate credential rotation for all shared or federated accounts using D3-CRO (Credential Rotation). Enforce MFA on all externally exposed applications per CIS 6.3. Restrict data access to least-privilege roles per NIST AC-6 (Least Privilege) and D3-UAP (User Account Permissions). Remove or disable any dormant accounts per CIS 5.3 (Disable Dormant Accounts — 45-day threshold).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-7 (Unsuccessful Logon Attempts), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For credential rotation without enterprise tooling: (1) Generate a list of all service accounts and user accounts with any Strategic Education integration permissions using 'net user /domain' or 'Get-ADUser -Filter * -Properties LastLogonDate, MemberOf | Where-Object {$_.MemberOf -match "StrategicEd|Strayer|Capella"}' and force password resets via 'Set-ADAccountPassword'. (2) For MFA enforcement on externally exposed applications without enterprise IdP budget, enable built-in MFA on your application (e.g., Microsoft 365 per-user MFA via admin portal, or Google Workspace 2-Step Verification enforcement in Admin Console — both free). (3) Identify dormant accounts (no logon in 45+ days) with: 'Search-ADAccount -AccountInactive -TimeSpan 45.00:00:00 | Disable-ADAccount' — run in report mode first, then execute with IR lead approval.

Evidence: Before rotating credentials: (1) Export a full dump of Active Directory or IdP last-logon timestamps for all accounts with Strategic Education integration roles — this baseline proves which accounts were active during the February 23–25 window and establishes the dormancy threshold for CIS 5.3 enforcement; (2) Capture current group membership and role assignments for all service accounts tied to Strategic Education APIs before modification — this preserves the pre-eradication access state for forensic and litigation purposes given active class action investigation; (3) If credential stuffing or account takeover is suspected as the breach vector, collect failed authentication logs (Event ID 4625) for the 72-hour window February 21–24, 2026 showing source IPs and targeted usernames before those logs age out of retention.

Step 4: Recovery — Validate that all third-party data connections to Strategic Education systems are documented and access-controlled per NIST AC-20. Confirm audit logging is intact and generating complete records per NIST AU-3 (Content of Audit Records) and AU-12 (Audit Record Generation). Run a privilege access review against NIST AC-6 and AC-2 (Account Management) to confirm no unauthorized accounts remain active. Monitor for downstream identity fraud indicators — particularly synthetic identity use of SSN + government ID combinations — over the next 90 days.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), NIST AU-3 (Content Of Audit Records), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For 90-day downstream fraud monitoring without commercial identity monitoring tools: (1) Subscribe your organization's security alias to HIBP (haveibeenpwned.com) domain notifications and to the Maine, Massachusetts, and Texas AG breach notification portals for any secondary disclosures related to this incident. (2) Configure a free osquery scheduled query on all endpoints handling student/HR data to detect anomalous file reads on SSN-containing data stores: query 'file_events' table for reads on known PII file paths by processes other than the authorized application. (3) For logging integrity verification, run 'Get-WinEvent -ListLog Security | Select-Object LogName, IsEnabled, FileSize, MaximumSizeInBytes' to confirm Security log capacity (cross-reference NIST AU-4 Audit Storage Capacity) has not been silently reduced — a common anti-forensic technique if an adversary had persistent access.

Evidence: Before closing recovery phase: (1) Generate and preserve a complete account inventory export (AD, cloud IdP, application-layer accounts) with current privilege assignments — this serves as the clean-baseline artifact for any future unauthorized-access claims; (2) Verify audit log continuity by checking for gaps in Windows Security Event Log sequence numbers or cloud audit log timestamps covering the February 23–25 breach window — log gaps are material evidence in the active class action litigation context and must be documented; (3) Capture network flow baselines (NetFlow or firewall log summaries) from the post-containment environment to establish a clean-state reference for anomaly detection during the 90-day monitoring window.

Step 5: Post-Incident — This breach exposes gaps in third-party data governance and government identifier handling. Conduct a formal review of data inventory per CIS 3.2 (Establish and Maintain a Data Inventory) to identify where SSNs and government IDs are stored, transmitted, or shared. Assess data access control lists per CIS 3.3. Review external system authorization policies under NIST AC-20. Implement or audit data minimization practices — government identifiers should not be retained beyond operational necessity (NIST AC-23, Data Mining Protection). Prepare regulatory response documentation for any state breach notification obligations applicable to your organization's student or customer population.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-23 (Data Mining Protection), NIST AU-11 (Audit Record Retention), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.3 (Configure Data Access Control Lists), CIS 3.4 (Enforce Data Retention), CIS 3.5 (Securely Dispose of Data), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For data inventory and minimization without enterprise DLP tooling: (1) Run a filesystem scan using 'grep -rE "\b[0-9]{3}-[0-9]{2}-[0-9]{4}\b" /path/to/data/' (Linux) or use the free tool 'PolySwarm Canary' or 'grep' equivalents via PowerShell ('Select-String -Path C:\DataShare* -Pattern "\b\d{3}-\d{2}-\d{4}\b" -Recurse') to locate unencrypted SSN-pattern data at rest. (2) Use ClamAV with a custom YARA rule targeting SSN and passport number regex patterns to scan shared drives and email archives for government identifier data that should be purged under CIS 3.5. (3) Document all findings in a data flow diagram updated to reflect Strategic Education data-sharing touchpoints — this diagram is your primary artifact for state breach notification assessments under Texas HB 4181, Massachusetts 201 CMR 17.00, and Maine 10 MRSA §1347.

Evidence: Preserve for post-incident record and potential regulatory review: (1) A point-in-time export of all data access control lists (ACLs/permissions) for repositories containing SSN and government ID data — this documents the pre-remediation access exposure scope for Maine, Massachusetts, and Texas breach notification obligations; (2) Retention schedule documentation showing how long SSNs and government IDs were held beyond operational necessity — directly relevant to AC-23 data minimization findings and litigation discovery requests from active class action investigation; (3) The complete incident timeline log with timestamps of detection, containment actions, and notification decisions — Maine, Massachusetts, and Texas each impose specific notification deadlines (30 days in Maine, as soon as reasonably possible in Massachusetts, 60 days in Texas) and this record demonstrates compliance or documents good-faith effort.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes, URLs) have been publicly released for this incident. Detection must focus on behavioral indicators aligned to mapped ATT&CK techniques. For T1078 (Valid Accounts): query authentication logs for logins from unexpected geographic locations, off-hours access, or accounts associated with Strategic Education federated identity. For T1530 (Data from Cloud Storage): alert on large-volume reads or exports from cloud storage buckets tied to student or customer PII datasets, particularly unusual API calls to storage services outside normal business hours. For T1005 (Data from Local System): monitor endpoint agents for bulk file access or compression events on systems housing government identifier datasets. For T1657 (Financial Theft): watch downstream fraud indicators in financial systems that consume SSN data. Log sources to prioritize: cloud storage access logs, identity provider authentication logs, DLP (Data Loss Prevention) alerts, and SIEM correlation rules for bulk PII access events. CIS 8.2 compliance (Collect Audit Logs) is a prerequisite, confirm logging is enabled on all systems touching government identifier data before tuning detection rules. Apply system file analysis and local account monitoring for systems storing SSN and government ID data.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1657** — Financial Theft
- **T1005** — Data from Local System

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **AC-3** — Access Enforcement

OWASP-TOP10-2021

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

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
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

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

ISO-27001-2022

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

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
T1657	Financial Theft	Impact
T1005	Data from Local System	Collection

Sources

Source	URL	Tier
gemini	https://www.classaction.org/news/strategic-education-data-breach-af...	T3
Strategic Education Inc.	https://www.strategiceducation.com/	T3

Source	URL	Tier
Strategic Education Data Breach Exposes Social Security Numbers	https://www.claimdepot.com/data-breach/strayer-university-2026	T3
[PDF] STRATEGIC EDUCATION, INC.	https://s203.q4cdn.com/245423802/files/doc_financials/2022/q4/2893b...	T3
Strategic Education Inc. Breach Investigation – Class Action Litigation	https://slfla.com/data-breach/strategic-education-inc-breach-invest...	T3

Generated 2026-06-04 19:24 UTC by TJS Security Command Center