INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:12 UTC

ShinyHunters-Linked Data Breach Exposes 2.3 Million Moody Bible Institute Accounts

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0214
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Moody Bible Institute, user account database (2.3 million accounts)
Published	2026-07-06
Discovery Source	Gemini

Executive Summary

Moody Bible Institute has confirmed a data breach in which personal information from over 2.3 million user accounts was published online. The incident has been corroborated by the institution's own investigation page, covered by The Register, and listed as a named breach in Have I Been Pwned. The breach carries reputational, regulatory, and downstream phishing risk for the institution and any affiliated organization whose users appear in the exposed dataset.

Technical Analysis

Moody Bible Institute confirmed unauthorized access to its user account database resulting in exposure of personal information across approximately 2.3 million accounts. The breach has been attributed in secondary reporting to actors linked to the ShinyHunters extortion group (MEDIUM confidence, named in secondary sources; no verified forensic statement from this source set). The initial access vector, specific compromised data fields, and full technical scope have not been independently confirmed in the available source material. Mapped weaknesses: CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) and CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor). Relevant MITRE ATT&CK techniques include T1530 (Data from Cloud Storage), T1657 (Financial Theft, reported in context of ShinyHunters extortion tradecraft), and T1589 (Gather Victim Identity Information). No CVE identifier is associated with this incident. Patch status is not applicable; the institution has published an incident investigation page at https://www.moody.edu/about/public-safety/.

Action Checklist

1. Containment, If your organization has any federated, SSO, or data-sharing relationship with Moody Bible Institute, suspend or review those trust relationships immediately and audit any shared user identity stores for overlap with the exposed population.
2. Detection, Query your SIEM for authentication events, password reset requests, or account enumeration patterns originating from email domains associated with Moody Bible Institute users (AU-2, AU-6). Cross-reference your user directory against Have I Been Pwned's named breach entry for MoodyBibleInstitute to identify any staff or affiliate accounts in the exposed dataset.
3. Eradication, No patch is applicable to third-party organizations. If internal accounts are confirmed in the breach, force password resets for those accounts and revoke any active sessions or API tokens associated with them (AC-2, CIS 5.2, D3-CRO).
4. Recovery, Enforce MFA for any accounts confirmed or suspected to be in the exposed dataset before restoring normal access (CIS 6.3, CIS 6.5, D3-MFA). Monitor those accounts for anomalous login behavior, privilege escalation attempts, and unusual data access for a minimum of 30 days post-reset (AC-2, AU-6, D3-LAM).
5. Post-Incident, Review third-party data-sharing agreements and vendor access inventories to assess exposure from future partner breaches (AC-20, CIS 3.2). Document this event as a case study for identity hygiene controls, including dormant account policies (CIS 5.3) and account inventory maintenance (CIS 5.1), and update playbooks accordingly.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and privacy officer if any confirmed internal accounts belong to employees with access to regulated data (FERPA, HIPAA, or state PII statutes), or if credential reuse is detected in authentication logs within your environment, as either condition triggers mandatory breach notification assessment timelines.
Recovery Notes	After completing password resets and MFA enforcement for all accounts confirmed or suspected in the MoodyBibleInstitute HIBP dataset, maintain a dedicated 30-day monitoring window targeting those specific accounts for Event IDs 4625, 4648, 4672, and 4732 — ShinyHunters-linked breach data is frequently sold to credential-stuffing operators who begin automated reuse attempts within days of public listing. Verify that no API tokens, OAuth refresh tokens, or long-lived service account credentials associated with the exposed accounts remain active, as these are not invalidated by a password reset alone. At day 30, conduct a formal account access review comparing current group memberships and access privileges against the pre-incident baseline captured during the eradication phase.

Forensic Artifacts	Identity provider authentication logs (Azure AD Sign-in logs, Okta System Log, or ADFS Event IDs 1200/1202) filtered for moody.edu-domain accounts — will show credential-stuffing attempts using the exposed plaintext or hashed credentials from the breach dataset in the days following its public HIBP listing | Windows Security Event Log Event ID 4648 (logon with explicit credentials) and 4776 (NTLM credential validation) for affected accounts — ShinyHunters breach data is commonly reused in pass-the-hash and credential-stuffing campaigns targeting enterprise environments where victims reuse passwords | Application-layer access logs for any externally exposed portals, VPNs, or APIs that accept authentication from moody.edu-affiliated accounts — specifically HTTP 200 responses following prior 401/403 sequences indicating successful credential reuse after multiple failures | Account password reset and session revocation audit trail from your identity provider, timestamped to document the window between breach public disclosure and your organization's remediation actions — relevant for regulatory breach notification timeline reconstruction | Have I Been Pwned breach record for MoodyBibleInstitute (haveibeenpwned.com/PwnedWebsites) preserved as a point-in-time screenshot or export, documenting the breach date, data classes exposed (email addresses, passwords, names, and any additional PII fields listed), and the size of the exposed population (2.3 million accounts) for your incident record

Per-Action IR Details

Containment — If your organization has any federated, SSO, or data-sharing relationship with Moody Bible Institute, suspend or review those trust relationships immediately and audit any shared user identity stores for overlap with the exposed population.

NIST Phase: Containment

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-3 (Access Enforcement), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without enterprise IAM tooling, query Active Directory or LDAP for any accounts provisioned via federated trust with moody.edu or affiliated domains: `Get-ADUser -Filter {UserPrincipalName -like '*moody.edu'} | Select Name,UserPrincipalName,Enabled`. Cross-reference your local user directory export (CSV) against the HIBP breach record for MoodyBibleInstitute using a free HIBP bulk-check script (e.g., HIBP-Checker on GitHub) — do not submit raw credentials, hash-compare only.

Evidence: Before suspending federated trust relationships or revoking SSO tokens, capture: current active SSO session logs from your identity provider (e.g., Azure AD Sign-in logs, Okta System Log, ADFS event logs — Windows Event IDs 1200/1202 for ADFS token issuance); a point-in-time export of all accounts with active federation grants to moody.edu or its affiliated domains; and any audit trail of recent cross-organizational data-sharing API calls. These records are transient and will be lost or overwritten once trust is suspended.

Detection — Query your SIEM for authentication events, password reset requests, or account enumeration patterns originating from email domains associated with Moody Bible Institute users (AU-2, AU-6). Cross-reference your user directory against Have I Been Pwned's named breach entry for MoodyBibleInstitute to identify any staff or affiliate accounts in the exposed dataset.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following PowerShell query against Windows Security Event Log for authentication anomalies tied to moody.edu-domain accounts: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4625,4648,4768,4771) -and $_.Message -match 'moody'} | Select TimeCreated,Id,Message | Export-Csv

moody_auth_events.csv`. For password reset activity, query Event ID 4723 (account password change attempt) and 4724 (admin-initiated reset). Use HIBP's free domain search (haveibeenpwned.com/DomainSearch) with your organization's domain to identify any staff email addresses in the MoodyBibleInstitute breach dataset.

Evidence: This is an analysis step that does not alter live state; no pre-capture is required. Collect and preserve: Windows Security Event Log entries for Event IDs 4625 (failed logon), 4648 (explicit credential logon), 4720 (account creation), 4723/4724 (password resets), and 4776 (credential validation) filtered for moody.edu-affiliated accounts; authentication logs from any external-facing application (VPN, webmail, portal) for the same account population; and the raw HIBP breach dataset entry for MoodyBibleInstitute to document the confirmed overlap at a point in time.

Eradication — No patch is applicable to third-party organizations. If internal accounts are confirmed in the breach, force password resets for those accounts and revoke any active sessions or API tokens associated with them (AC-2, CIS 5.2, D3-CRO).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords)

Compensating: Without enterprise PAM tooling, force password resets via PowerShell: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText 'TempP@ss!2026' -Force); Set-ADUser -Identity -ChangePasswordAtLogon $true`. Revoke active web application sessions by invalidating session tokens directly in the application database or by cycling the application's session secret. Enumerate and revoke API tokens by searching your token store or `.env` configurations for credentials associated with the confirmed accounts.

Evidence: Before forcing password resets or revoking sessions/API tokens — actions that destroy live authentication state — capture: a current export of all active sessions for the affected accounts from your identity provider or application session store (e.g., `Get-PSSession`, Azure AD `Get-AzureADUserRegisteredDevice`, or application-specific session tables); a list of all API tokens, OAuth grants, and refresh tokens issued to or by the affected accounts; and Windows Security Event Log Event ID 4627 (group membership enumeration) and 4672 (special privileges assigned) for those accounts to assess any privilege abuse that occurred during the window of exposure while credentials were compromised.

Recovery — Enforce MFA for any accounts confirmed or suspected to be in the exposed dataset before restoring normal access (CIS 6.3, CIS 6.5, D3-MFA). Monitor those accounts for anomalous login behavior, privilege escalation attempts, and unusual data access for a minimum of 30 days post-reset (AC-2, AU-6, D3-LAM).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Without enterprise MFA infrastructure, enforce MFA via Microsoft Authenticator (free Azure AD MFA for up to 50 users on the free tier) or Google Authenticator integrated with a free TOTP-capable identity provider (e.g., Authelia, Keycloak). For the 30-day monitoring window without a SIEM, create a scheduled PowerShell task that runs nightly and exports Event IDs 4625, 4648, 4672, and 4732 (member added to security group) for the affected account list to a CSV reviewed each morning by the two-person team: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4625,4648,4672,4732)} | Export-Csv -Append daily_watch_$(Get-Date -Format yyyyMMdd).csv`.

Evidence: Before restoring normal access to any account in the confirmed or suspected exposed population, verify and document: completion of the credential revocation step (session tokens invalidated, API tokens rotated); confirmation that MFA enrollment is active and tested for each account being re-enabled; and a baseline snapshot of each account's current group memberships, assigned roles, and recent access history (last 30 days) against which the 30-day monitoring window will be compared to detect post-recovery privilege escalation or lateral movement originating from a ShinyHunters-linked credential reuse attempt.

Post-Incident — Review third-party data-sharing agreements and vendor access inventories to assess exposure from future partner breaches (AC-20, CIS 3.2). Document this event as a case study for identity

hygiene controls, including dormant account policies (CIS 5.3) and account inventory maintenance (CIS 5.1), and update playbooks accordingly.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use Of External Systems), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Without a GRC platform, maintain third-party access inventories in a structured spreadsheet tracking: vendor/partner name, data-sharing scope, federated access type, last access review date, and breach notification contact. For dormant account identification, run a scheduled monthly PowerShell audit: `Search-ADAccount -AccountInactive -TimeSpan 45.00:00:00 -UsersOnly | Select Name,LastLogonDate,Enabled | Export-Csv dormant_accounts_$(Get-Date -Format yyyyMMdd).csv`. Use the ShinyHunters/MoodyBibleInstitute incident as the documented trigger case for updating your third-party breach response playbook.

Evidence: This post-incident phase does not alter live system state; no pre-capture is required. Collect and preserve as institutional documentation: the full timeline of the MoodyBibleInstitute breach disclosure (HIBP listing date, The Register coverage date, institution investigation page publication date) to anchor your lessons-learned record; the final list of internal accounts confirmed or suspected in the exposed dataset with their resolution status (reset, revoked, monitored, cleared); and the pre-existing state of your third-party data-sharing agreements and federated access inventory at the time of breach discovery, to serve as the baseline against which improvements will be measured.

Detection Guidance

Query Have I Been Pwned's API or breach search (https://haveibeenpwned.com/Breach/MoodyBibleInstitute) to identify whether any organizational email addresses appear in the Moody Bible Institute breach entry. In your SIEM, search authentication logs for accounts matching exposed email domains for anomalous login times, impossible travel, or credential stuffing patterns (multiple failed logins followed by success). Monitor for inbound phishing campaigns targeting staff using personal details consistent with the leaked data types, name and email combinations are sufficient for convincing spear-phishing. No specific IOC hashes, IPs, or domains have been confirmed in the available source material for this incident.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1657** — Financial Theft
- **T1589** — Gather Victim Identity Information

OWASP-TOP10-2021

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

NIST-800-53R5

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

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

SOC2-TSC

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

ISO-27001-2022

- **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
T1657	Financial Theft	Impact
T1589	Gather Victim Identity Information	Reconnaissance

Sources

Source	URL	Tier
Moody Bible Institute breach leaves 2.3M accounts needing ...	https://www.theregister.com/security/2026/07/06/moody-bible-institu...	T2
Public Safety | Moody Bible Institute	https://www.moody.edu/about/public-safety/	T1
Moody Bible Institute Data Incident Investigation	https://www.moodybible.org/news/2026/data-investigation/	T3
Moody Bible Institute Data Breach - Have I Been Pwned	https://haveibeenpwned.com/Breach/MoodyBibleInstitute	T3

Generated 2026-07-06 15:12 UTC by TJS Security Command Center