INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:36 UTC

Marquis Data Breach Affects 672,000 Individuals via Ransomware Attack

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0057
Type	Data Breach
Severity	HIGH
Affected Products	Marquis (organization), customer and individual personal and financial data
Published	2026-03-20

Executive Summary

Marquis disclosed a ransomware attack that exposed personal and financial data belonging to approximately 672,000 individuals, revised downward from an initial estimate of 1.6 million. The stolen data includes sensitive personal and financial information, creating direct regulatory exposure under applicable breach notification laws and significant reputational risk. Organizations with Marquis as a vendor or data-sharing partner should assess third-party data flow agreements and monitor for downstream fraud activity affecting shared customers.

Technical Analysis

Marquis sustained a ransomware attack resulting in confirmed data exfiltration prior to encryption, consistent with double-extortion tradecraft. The incident maps to CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques associated with this incident pattern include T1486 (Data Encrypted for Impact), T1078 (Valid Accounts, likely used for initial access or lateral movement), and T1566 (Phishing, common ransomware delivery vector). No CVE has been assigned; this is a breach incident, not a software vulnerability disclosure. No CVSS score applies. The victim count was revised from 1.6 million to 672,000 in March 2026, suggesting ongoing forensic scope refinement. No specific IOCs, ransomware variant, or initial access vector have been publicly confirmed as of available reporting.

Action Checklist

1. Step 1, Immediate: Determine whether your organization shares data with Marquis or uses Marquis services; identify any affected data flows involving personal or financial records.
2. Step 2, Detection: Review email gateway and endpoint logs for phishing indicators and anomalous authentication events (Valid Accounts, T1078) against Marquis-connected systems or shared identity

providers.

3. Step 3, Assessment: Inventory third-party data sharing agreements with Marquis; confirm what categories of personal and financial data were in scope and whether your organization's customer or employee records are included in the 672,000 affected individuals.

4. Step 4, Communication: If affected data is confirmed, engage legal and compliance teams to assess breach notification obligations under applicable regulations (e.g., state breach notification laws, GLBA, HIPAA if applicable); notify affected individuals per regulatory timelines.

5. Step 5, Long-term: Review third-party vendor risk assessments for ransomware resilience controls; verify contractual data breach notification SLAs with vendors; update incident response playbooks to address third-party ransomware scenarios with exfiltration components.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO/General Counsel immediately upon confirming any overlap between affected Marquis individuals and your customer/employee base; escalate to external IR firm or forensic vendor if your organization lacks capability to audit third-party data access logs or perform breach scope analysis within 24 hours.
Recovery Notes	Post-containment: (1) Work with Marquis to obtain forensic report detailing what data was exfiltrated, when, and by which threat actor (if known); cross-reference against your inventory to confirm final scope. (2) Reset credentials for any service accounts that accessed Marquis systems, revoke API tokens, and review IAM logs for privilege escalation or lateral movement attempts. (3) For customers whose data was exposed, provide 2–3 years of complimentary credit monitoring and consider reputation recovery activities (transparency reports, customer communication, board notification). (4) Conduct post-incident review with forensic findings and update vendor risk management process; establish annual vendor ransomware resilience re-assessment cadence.
Forensic Artifacts	Windows Event Security Log (Event ID 4624, 4625, 4688, 4720, 4722, 4769) — authentication, process creation, account creation | Email gateway message tracking logs and quarantine records — phishing attack vector and lateral movement via email compromise | DNS query logs and web proxy access logs — command-and-control (C2) communication and data exfiltration destinations | Database transaction logs (SQL Server, Oracle, PostgreSQL) and API audit logs — data access patterns and volumetric anomalies indicating bulk exfiltration | VPN access logs and Marquis integration service account logs — entry point and privilege escalation path during initial compromise

Per-Action IR Details

Step 1 — Immediate: Determine whether your organization shares data with Marquis or uses Marquis services; identify any affected data flows involving personal or financial records.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase emphasizes asset inventory and third-party dependencies)

Controls: NIST 800-53 SA-9 (Third-Party System Services), NIST 800-53 IA-4 (Identifier Management), CIS 6.1 (Inventory of Authorized and Unauthorized Software)

Compensating: Query Active Directory for service accounts tied to Marquis integration; grep firewall logs for outbound connections to Marquis IP ranges (obtain from vendor); search email archive for Marquis-related contracts or service agreements using keyword search ('Marquis', 'vendor', 'data sharing'); manually audit data classification tags or labels

in shared folders matching PII/financial categories.

Evidence: Capture before executing: (1) Screenshot or export of current third-party vendor registry or CMDB; (2) Active Directory user/service account export (Get-ADUser -Filter * -Property *); (3) Network firewall allow rules and DNS resolution logs for Marquis domains; (4) Email archive metadata showing data-sharing agreements or contract terms; (5) Current data flow diagrams or DLP policy matches if available.

Step 2 — Detection: Review email gateway and endpoint logs for phishing indicators and anomalous authentication events (Valid Accounts, T1078) against Marquis-connected systems or shared identity providers.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and analysis; emphasis on analyzing logs and alert sources to confirm incident)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 IA-2 (Authentication), CIS 8.2 (Audit Log Centralization)

Compensating: Without SIEM: (1) Export email gateway logs (most email appliances export CSV via admin console) and filter for Marquis sender domains or keywords 'urgent', 'verify account', 'confirm password'; (2) Query Windows Event Log 4625 (failed logons) and 4624 (successful logons) on domain controllers using 'wevtutil qe Security /q:"Event[System/EventID=4624]" /format:csv > logins.csv'; (3) On endpoints, use 'Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4688}' to export process creation logs and look for cmd.exe, powershell.exe, net.exe with unusual parameters; (4) Check email logs for forwarding rules: 'Get-Mailbox -ResultSize Unlimited | Get-InboxRule | where {$_.ForwardTo -ne $null}'.

Evidence: Capture immediately (do NOT delete after analysis): (1) Email gateway quarantine logs or message tracking for 30 days prior; (2) Windows Event Security logs (Event ID 4624, 4625, 4688, 4720, 4722) for Marquis-related accounts; (3) VPN access logs if Marquis access requires VPN; (4) DNS query logs showing resolution to suspicious domains; (5) Endpoint EDR agent telemetry (process creation, network connections, file modifications) for any Marquis-connected systems; (6) Web proxy logs for data exfiltration indicators (large file uploads to cloud storage, uncommon file types).

Step 3 — Assessment: Inventory third-party data sharing agreements with Marquis; confirm what categories of personal and financial data were in scope and whether your organization's customer or employee records are included in the 672,000 affected individuals.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Analyzing incident scope and impact to determine whether response escalation is warranted)

Controls: NIST 800-53 SA-9 (Third-Party System Services), NIST 800-53 SA-3 (System Development Life Cycle), CIS 6.2 (Address Unauthorized Software)

Compensating: Without a formal asset inventory: (1) Search contract management system or shared drives for any document containing 'Marquis' and data classification terms; (2) Query database schema documentation and data lineage logs to identify tables containing PII (SSN, tax ID, financial account numbers, names+addresses); (3) Cross-reference customer/employee master lists against Marquis user directories or API logs to determine overlap; (4) Interview business unit leads responsible for Marquis integration to document data category (names, account numbers, medical records, etc.) and record count; (5) Run SQL queries against source databases: 'SELECT COUNT(DISTINCT customer_id) FROM [table] WHERE data_shared_with_vendor = 'Marquis''.

Evidence: Preserve before proceeding: (1) All signed data sharing agreements, BAAs (Business Associate Agreements), or vendor contracts; (2) Database schema exports showing PII field definitions; (3) Access logs or audit trails showing what data was accessed by Marquis service accounts (query logs, API call logs); (4) DLP policy match reports if data to Marquis is monitored; (5) Customer/employee master data exports (hashed or anonymized for privacy) to enable overlap analysis; (6) Screenshot of current data flow diagram showing Marquis touchpoints.

Step 4 — Communication: If affected data is confirmed, engage legal and compliance teams to assess breach notification obligations under applicable regulations (e.g., state breach notification laws, GLBA, HIPAA if

applicable); notify affected individuals per regulatory timelines.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-incident activities, specifically public notification and regulatory reporting)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-6 (Incident Reporting), CIS 17.1 (Incident Response and Reporting)

Compensating: Without legal team: (1) Consult state-specific breach notification laws using free resources (National Conference of State Legislatures NCSL template or state AG website); (2) If GLBA applies, review 16 CFR Part 682.2 for notification timeline (without unreasonable delay, typically 30–60 days); (3) Use notification template from state AG office or SANS Institute breach notification guide; (4) Maintain signed evidence that notifications were sent (email delivery receipts, certified mail proof, phone tree logs); (5) Document regulatory authority contact (state AG, FTC, relevant HIPAA Regional Office if applicable) and submission date; (6) Create incident timeline document referencing Step 1–3 findings as evidence of due diligence.

Evidence: MUST capture before sending notifications: (1) Forensic report confirming which specific data categories were exposed (cross-reference Step 3 data inventory with Marquis public disclosure); (2) Complete list of affected individuals with notification addresses (email, mailing address, phone); (3) Breach notification letter template reviewed and approved by legal; (4) Evidence of law enforcement notification if required (police report number, FBI IC3 report); (5) Proof of notification delivery for regulatory audit trail; (6) Communications log showing decision points and timeline.

Step 5 — Long-term: Review third-party vendor risk assessments for ransomware resilience controls; verify contractual data breach notification SLAs with vendors; update incident response playbooks to address third-party ransomware scenarios with exfiltration components.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4.1 (Lessons learned; emphasis on improving processes and controls post-incident)

Controls: NIST 800-53 SA-9 (Third-Party System Services), NIST 800-53 SA-12 (Supply Chain Risk Management), NIST 800-53 IR-2 (Incident Response Training), CIS 17.7 (Test Incident Response Plan)

Compensating: Without enterprise vendor risk platform: (1) Use NIST SP 800-53 SA-9 control checklist to create a vendor assessment questionnaire (Ransomware resilience questions: backup strategy, recovery time objective, encryption practices, incident notification SLA, insurance coverage); (2) Send questionnaire to top 10–20 vendors; track responses in spreadsheet with yes/no/unknown status; (3) Identify vendors with ransomware response SLA in contract — if missing, prepare amendment template requiring notification within 24–72 hours of confirmed breach; (4) Develop free IR playbook template using NIST 800-61r3 Table 1 (phases) and ATT&CK-mapped detection rules; map exfiltration paths specific to data-sharing vendors (S3 bucket access, API token misuse, database export logs); (5) Host tabletop exercise with cross-functional team (IT, security, legal, comms) using Marquis scenario to validate playbook; document findings and update annually.

Evidence: Document for post-incident closure: (1) Current vendor risk assessment spreadsheet with Marquis entry flagged as 'ransomware + exfiltration'; (2) Updated data sharing agreements with revised SLAs for breach notification (timelines, escalation contacts, insurance verification); (3) Revised IR playbook with sections for third-party breach containment (who to contact at vendor, how to revoke API tokens, data recovery procedures); (4) Tabletop exercise attendee sign-off and action items log; (5) Notification to board/management summarizing control gaps and remediation timeline.

Detection Guidance

No confirmed IOCs have been publicly released for this incident. Detection should focus on behavioral and contextual indicators consistent with the mapped ATT&CK techniques. Check identity provider and VPN logs for anomalous authentication from Marquis-associated accounts or shared SSO integrations (T1078). Review email security logs for phishing delivery attempts targeting Marquis or connected supply chain contacts (T1566). If your organization has direct network connectivity to Marquis environments, inspect firewall and proxy logs for unusual outbound data transfers preceding the disclosed incident window. Monitor dark web and breach

notification services (e.g., HaveIBeenPwned, CISA alerts) for emergence of Marquis data in credential dumps. Given the double-extortion pattern implied by data theft plus encryption, any future ransomware group claims referencing Marquis should be treated as potentially containing exfiltrated data usable for spear-phishing or fraud against affected individuals.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not-confirmed`	No IOCs publicly disclosed for this incident as of March 2026 reporting. Monitor threat intelligence feeds for ransomware group claims referencing Marquis.	LOW

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1657** — Financial Theft

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

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

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

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
	https://www.securityweek.com/marquis-data-breach-affects-672000-ind...	T3
Marquis says over 672,000 people had personal and financial data ...	https://techcrunch.com/2026/03/18/marquis-says-over-672000-people-h...	T2
Marquis confirms sensitive personal data of 672000 people stolen in ...	https://www.techradar.com/pro/security/marquis-confirms-sensitive-p...	T3
Marquis says over 672000 people had personal and financial data ...	https://www.reddit.com/r/texas/comments/1ryejzx/marquis_says_over_6...	T3
Marquis Data Breach Affects 672,000 Individuals - SecurityIT	https://www.show.it/en/marquis-data-breach-affects-672000-individuals/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:36 UTC by TJS Security Command Center