INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-04-03 06:20 UTC

Marquis Fintech Ransomware Attack Exposes 672,000 Bank Customer Records

DATA BREACH | HIGH | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0075
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Marquis (Texas-based fintech/banking technology firm), customer data systems
Published	1 day ago
Discovery Source	Serper

Executive Summary

Texas-based banking technology provider Marquis suffered a ransomware attack in 2025 that exfiltrated sensitive records for over 672,000 individuals, including names, physical addresses, and payment card numbers. Because Marquis operates as a third-party technology provider to financial institutions, the breach creates downstream supply-chain exposure for any bank or credit union relying on Marquis systems. Business risk centers on regulatory notification obligations, potential card fraud liability, and reputational damage for affected financial institution clients.

Technical Analysis

Marquis, a Texas-based fintech and banking technology firm, confirmed a ransomware attack that resulted in data exfiltration affecting 672,000+ individuals. Stolen data includes names, physical addresses, and payment card numbers, categories that trigger PCI DSS breach notification and state-level financial privacy statutes. No CVE has been assigned; this is an organizational breach, not a disclosed software vulnerability. CWE-693 (Protection Mechanism Failure) is the closest applicable weakness classification, reflecting a failure of controls designed to prevent unauthorized access and data exfiltration. MITRE ATT&CK techniques observed or consistent with this incident type include: T1566 (Phishing, likely initial access vector), T1078 (Valid Accounts, credential abuse for persistence or lateral movement), T1486 (Data Encrypted for Impact, ransomware payload), T1485 (Data Destruction, potential secondary payload), and T1041 (Exfiltration Over C2 Channel, data theft prior to encryption). No specific threat actor group has been confirmed. Patch status is not applicable; remediation requires organizational and third-party vendor controls review. Source quality is Tier 3 (trade and general press); no official Marquis advisory or regulatory filing has been confirmed in available sources.

Action Checklist

1. Step 1: Containment, Identify all data feeds, APIs, and integrations with Marquis systems. Suspend or isolate connections to Marquis environments until the company confirms remediation scope. Inventory which customer records your institution contributed to Marquis data stores.
2. Step 2: Detection, Query your SIEM and DLP logs for outbound data transfers to Marquis-associated endpoints over the past 12 months. Review access logs for any shared credentials or SSO tokens scoped to Marquis integrations. Check endpoint detection telemetry on systems with Marquis connectivity for T1078 (anomalous valid account usage) and T1041 (unusual outbound transfer volumes).
3. Step 3: Eradication, Rotate all credentials, API keys, and service account tokens used to authenticate to Marquis systems. Revoke and reissue any shared secrets. If your institution contributed payment card data to Marquis, coordinate with your card brand (Visa, Mastercard) on potential card block and reissue workflows per PCI DSS Incident Response requirements.
4. Step 4: Recovery, Validate that no active sessions or persistent connections to Marquis infrastructure remain. Monitor downstream fraud signals (card-not-present fraud, account takeover attempts) for customer cohorts whose data was in scope. Confirm with Marquis in writing the remediation steps taken and request evidence of restored control posture before reconnecting integrations.
5. Step 5: Post-Incident, Conduct a third-party vendor risk review. Evaluate whether Marquis and similar vendors meet your institution's vendor security requirements, including SOC 2 Type II, penetration testing cadence, and breach notification SLAs. Document control gaps in your vendor risk register and update your Third-Party Risk Management policy to require contractual breach notification timelines aligned with state financial privacy statutes and GLBA Safeguards Rule obligations.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and your primary federal regulator (OCC, FDIC, or NCUA as applicable) if your institution's customer PAN data is confirmed within the 672,000-record Marquis breach scope, as GLBA Safeguards Rule (16 CFR Part 314.15) requires notification to the Federal Trade Commission within 30 days of discovering a breach involving customer financial information, and Texas Business & Commerce Code §521 imposes state-level notification obligations to affected individuals.
Recovery Notes	Before restoring any Marquis integrations, require a written attestation from Marquis — supported by an executive summary from their forensic IR firm — confirming ransomware eradication, credential rotation, and restored endpoint integrity across all systems that processed your institution's customer data. Monitor card-not-present fraud and account takeover rates for the specific customer cohort whose records were in Marquis's custody for a minimum of 90 days post-discovery, as PAN monetization on dark web marketplaces typically lags exfiltration by 30–90 days. Maintain enhanced fraud monitoring thresholds for this cohort through the full card reissuance cycle — until replacement cards are issued and activated, displaced PANs remain exploitable.

Forensic Artifacts	Outbound firewall and proxy logs showing connection history to Marquis-associated IP ranges and hostnames over the 12 months preceding breach discovery — specifically byte-count anomalies on upload sessions consistent with bulk PAN and PII exfiltration preceding the ransomware deployment event | API gateway request/response logs for all Marquis-bound integration endpoints, preserving the specific data fields (PAN, name, address) transmitted per API call — these establish your institution's data-in-scope inventory and are essential for the individual notification count required by state breach statutes | SSO and IdP audit logs (Okta system log, Azure AD sign-in log, or equivalent) for all authentication events by Marquis-scoped service accounts, filtered for logon anomalies consistent with MITRE ATT&CK T1078 (Valid Accounts) — credential abuse is the primary lateral movement vector in ransomware supply-chain attacks against SaaS fintech providers | DLP platform alert history for outbound transfers matching PAN regex patterns (e.g., Luhn-valid 16-digit sequences) destined for Marquis endpoints — confirms whether your DLP controls detected but did not block the exfiltration, which is a GLBA Safeguards Rule control deficiency requiring disclosure to regulators | Card management system transaction and dispute logs for the specific BIN ranges and account numbers transmitted to Marquis, preserved as legal-hold evidence to support card brand (Visa/Mastercard) chargeback liability assessments and to establish the pre-breach fraud baseline needed to attribute post-breach card-not-present fraud losses

Per-Action IR Details

Step 1: Containment — Identify all data feeds, APIs, and integrations with Marquis systems. Suspend or isolate connections to Marquis environments until the company confirms remediation scope. Inventory which customer records your institution contributed to Marquis data stores.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without a network access control platform: immediately enumerate Marquis-bound connections using 'netstat -ano' on Windows or 'ss -tunp' on Linux on all systems with known Marquis integrations, then create host-based firewall deny rules for Marquis IP ranges using 'netsh advfirewall firewall add rule' (Windows) or 'iptables -I OUTPUT -d -j DROP' (Linux). Document each blocked connection with a timestamp and system hostname before severing. Use your network switch's ACL or VLAN segmentation to isolate any server segment that hosted Marquis API connectors.

Evidence: Before severing connections, capture: (1) full netflow or firewall connection-state logs showing active sessions to Marquis-associated IP ranges or hostnames (preserve these as timestamped exports — they establish scope of active exposure at time of discovery); (2) DNS query logs from your resolver for Marquis-related domains over the prior 12 months (identifies which internal hosts were communicating with Marquis infrastructure); (3) a snapshot of your API gateway or middleware configuration files showing which data fields — specifically payment card numbers and PII — were included in outbound data feeds to Marquis.

Step 2: Detection — Query your SIEM and DLP logs for outbound data transfers to Marquis-associated endpoints over the past 12 months. Review access logs for any shared credentials or SSO tokens scoped to Marquis integrations. Check endpoint detection telemetry on systems with Marquis connectivity for T1078 (anomalous valid account usage) and T1041 (unusual outbound transfer volumes).

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM: query Windows Security Event Log on Marquis-integrated servers for Event ID 4648 (explicit credential logon with Marquis service account names) and Event ID 4624 logon type 3 (network logon) filtering on accounts scoped to Marquis. On Linux, run 'grep -E "" /var/log/auth.log' and 'grep -E "POST|PUT" /var/log/nginx/access.log | awk "{print $1, $7, $10}" | sort -k3 -rn | head -100' to surface high-volume outbound API calls. Deploy Sysmon with SwiftOnSecurity's config and query for Event ID 3 (Network Connection) where the destination IP matches known Marquis CIDR blocks. For T1041 detection without EDR, use Wireshark with a capture filter of 'host and tcp.flags.push==1' on the integration server's NIC to identify bulk data transfer patterns.

Evidence: Before completing analysis: (1) export DLP policy hit logs filtered for 'payment card number' (PAN) pattern matches on outbound transfers to Marquis endpoints — these directly evidence which card records transited your systems to Marquis; (2) pull SSO provider audit logs (Okta, Azure AD, or equivalent) for all authentication events by service accounts scoped to Marquis applications, focusing on logon times outside business hours and source IPs deviating from expected integration server ranges (MITRE ATT&CK T1078 — Valid Accounts); (3) capture proxy or firewall logs showing byte counts on outbound connections to Marquis endpoints — ransomware operators typically exfiltrate before encrypting, so anomalous upload spikes preceding the publicly reported attack date are key evidence of the exfiltration stage (T1041 — Exfiltration Over C2 Channel).

Step 3: Eradication — Rotate all credentials, API keys, and service account tokens used to authenticate to Marquis systems. Revoke and reissue any shared secrets. If your institution contributed payment card data to Marquis, coordinate with your card brand (Visa, Mastercard) on potential card block and reissue workflows per PCI DSS Incident Response requirements.

NIST Phase: Eradication

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

Controls: NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without a PAM (Privileged Access Management) platform: generate a complete list of all service accounts, API keys, and OAuth tokens scoped to Marquis by running 'Get-ADServiceAccount -Filter * | Where-Object {$_.Description -like "*Marquis*"}' in PowerShell and cross-referencing your API gateway's credential store. Rotate each credential individually, confirm revocation in the identity provider's audit log (Event ID 4723 — Password Change Attempt, or Event ID 4726 — User Account Deleted for deprecated accounts), and store new secrets in a local KeePass vault with restricted file-system ACLs as an interim measure pending a secrets manager deployment. For card reissuance coordination, document the specific BIN ranges and card-present vs. card-not-present exposure to provide to Visa/Mastercard's fraud operations teams.

Evidence: Before rotating credentials: (1) export the full audit trail of API key last-used timestamps from your API gateway (Kong, AWS API Gateway, Apigee, or equivalent) — these establish whether Marquis credentials were accessed by unauthorized parties prior to rotation; (2) pull Active Directory or IdP logs for all password resets, token refreshes, and privilege escalation events on Marquis-scoped service accounts over the past 90 days; (3) capture your card management system's transaction logs for the specific PANs transmitted to Marquis, preserving these as legal-hold evidence to support card brand chargeback liability determinations and state breach notification filings.

Step 4: Recovery — Validate that no active sessions or persistent connections to Marquis infrastructure remain. Monitor downstream fraud signals (card-not-present fraud, account takeover attempts) for customer cohorts whose data was in scope. Confirm with Marquis in writing the remediation steps taken and request evidence of restored control posture before reconnecting integrations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-12 (Audit Record Generation), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a commercial fraud monitoring platform: configure your card processing platform's existing dispute and chargeback reporting to flag the specific BIN ranges and customer cohort account numbers exposed in the Marquis breach — most core banking platforms support custom alert thresholds on dispute velocity. For account takeover detection without enterprise UEBA, use osquery with a scheduled query against your authentication logs:

'SELECT * FROM last WHERE username IN () AND time > ' on Linux auth systems, or query Windows Security Event ID 4625 (Failed Logon) with a filter on the affected customer account population. Set a 90-day monitoring window given the typical lag between PAN exfiltration and card-not-present fraud monetization.

Evidence: Before reconnecting Marquis integrations: (1) obtain and retain Marquis's written remediation attestation and any supporting forensic report from their IR firm — this is a contractual and regulatory artifact, not merely a courtesy; (2) verify the absence of persistent connections by running a full port scan of your DMZ and integration server segments against known Marquis IP ranges using Nmap ('nmap -sT -p 443,8443,8080 ') and confirm zero established states; (3) pull your fraud operations platform's card-not-present dispute reports segmented by the affected customer cohort as a baseline — document the pre-reconnection fraud rate so any post-reconnection spike is attributable.

Step 5: Post-Incident — Conduct a third-party vendor risk review. Evaluate whether Marquis and similar vendors meet your institution's vendor security requirements, including SOC 2 Type II, penetration testing cadence, and breach notification SLAs. Document control gaps in your vendor risk register and update your Third-Party Risk Management policy to require contractual breach notification timelines aligned with state financial privacy statutes and GLBA Safeguards Rule obligations.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST CA-2 (Control Assessments), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a commercial vendor risk management (VRM) platform: build a Marquis-specific control gap worksheet in a spreadsheet mapping the GLBA Safeguards Rule's 16 CFR Part 314 requirements against Marquis's last-available SOC 2 Type II report findings — focus on the Security and Availability trust service criteria relevant to data custody. Use CISA's free 'Stakeholder Specific Vulnerability Categorization (SSVC)' decision tree methodology to prioritize remediation of the identified gaps by exploitability and mission impact. Draft a board-ready one-page incident summary documenting the breach timeline, customer record scope (672,000 individuals), data types exposed (names, addresses, PANs), and regulatory notification obligations under Texas Business & Commerce Code §521 and GLBA — this serves as the post-incident lessons-learned artifact required by NIST IR-8.

Evidence: After incident closure: (1) retain all Marquis-related vendor contracts, DPAs, and prior security questionnaire responses as evidence for regulatory examination — Texas DFPS, OCC, or FDIC examiners will request these during any supervisory review triggered by the breach; (2) preserve your institution's breach notification timeline documentation (discovery date, notification date, state AG filing) to demonstrate compliance with state financial privacy statute deadlines; (3) archive the completed vendor risk re-assessment against Marquis, including any SOC 2 Type II bridge letters or penetration test summaries obtained, as evidence that vendor due diligence was conducted post-incident.

Detection Guidance

No confirmed IOCs (IP addresses, domains, file hashes) have been publicly released for this incident as of available reporting. Detection should focus on behavioral indicators consistent with the mapped MITRE techniques. In your SIEM, query for: (1) anomalous authentication events against Marquis-integrated service accounts, flag T1078 patterns such as logins outside business hours, logins from new geographies, or privilege escalation on accounts scoped to Marquis. (2) Outbound data transfer spikes to external destinations from systems with Marquis connectivity, flag potential T1041 exfiltration patterns, particularly large POST or PUT requests or unusual SFTP/FTP sessions. (3) Any phishing-related detections (T1566) targeting staff with access to Marquis systems in the 30-90 days preceding the confirmed breach window. For downstream fraud detection, cross-reference your institution's card fraud monitoring system against the customer cohort whose records were held by Marquis. Prioritize CNP (card-not-present) fraud alerts and new account opening attempts using

affected PII combinations. Note: absence of published IOCs limits technical detection. Human verification of Marquis's incident disclosure and any regulatory filing (e.g., HHS, state AG, CFPB) is recommended before scoping your exposed population.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not-confirmed`	No IOCs have been publicly confirmed for this incident in available Tier 3 sources. Do not act on unverified indicators. Monitor Marquis's official communications and FS-ISAC for confirmed IOC releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1485** — Data Destruction
- **T1566** — Phishing
- **T1041** — Exfiltration Over C2 Channel

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
- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

- **GV.SC-01** — Cybersecurity supply chain risk management program

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1485	Data Destruction	Impact
T1566	Phishing	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
	https://www.foxnews.com/tech/banking-tech-data-breach-exposes-672k-...	T3
Banking tech data breach exposes 672K in ransomware attack - AOL	https://www.aol.com/articles/banking-tech-data-breach-exposes-17004...	T3
Marquis ransomware attack exposed 672,000 bank customer records	https://thepaypers.com/fraud-and-fincrime/news/marquis-discloses-ra...	T3
Marquis confirms cyberattack affecting 672K customers - LinkedIn	https://www.linkedin.com/news/story/marquis-confirms-cyberattack-af...	T3

Source	URL	Tier
Marquis says over 672,000 people had personal and financial data ...	https://www.msn.com/en-us/news/us/marquis-says-over-672-000-people-...	T3

Generated 2026-04-03 06:20 UTC by TJS Security Command Center