INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 15:55 UTC

Plaza Home Mortgage Data Breach Triggers Class Action Litigation

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0158
Type	Data Breach
Severity	HIGH
Affected Products	Plaza Home Mortgage, consumer and employee PII (breach disclosed May 2026, approximately 137,976 individuals affected)
Published	15 hours ago
Discovery Source	Serper

Executive Summary

Plaza Home Mortgage disclosed a data breach in May 2026 affecting approximately 137,976 consumers and employees whose personally identifiable information was exposed. The company now faces at least two class action lawsuits filed within roughly one month of the breach disclosure. Business risk is elevated: litigation costs, regulatory scrutiny from financial services regulators, and reputational damage in a trust-sensitive mortgage industry are all active.

Technical Analysis

No CVE has been assigned to this incident. The attack vector, technical root cause, and specific data types compromised have not been confirmed in available sources as of this writing. Affected population: approximately 137,976 individuals, including consumers and employees. Data exposure involves PII; precise field-level disclosure (e.g., SSNs, financial account numbers, dates of birth) has not been confirmed by the company in sources available at this time. No CVSS score, CWE classification, or MITRE ATT&CK technique mapping is possible without confirmed technical details. Source quality score is 0.64 (T3 tier sources only; no official company breach notification accessed), and all available sources are Tier 3 (news aggregators, class action trackers, social media). Human verification against Plaza Home Mortgage's official breach notification filing and any HHS/state AG notifications is required before operational use.

Action Checklist

1. Step 1: Awareness. Monitor Plaza Home Mortgage's official communications and any state Attorney General or CFPB breach notification filings for confirmed data types and root cause. Do not act on

unconfirmed scope.

2. Step 2: Detection. If your organization has a vendor or data-sharing relationship with Plaza Home Mortgage, review data exchange agreements and audit logs (NIST AU-6: Audit Record Review, Analysis, and Reporting; CIS 8.2: Collect Audit Logs) for any abnormal data access or exfiltration indicators involving Plaza systems or shared data sets.

3. Step 3: Eradication. No confirmed attack vector is available; no specific patch or configuration remediation can be specified at this time. Assign ownership for re-evaluation when Plaza Home Mortgage publishes official breach notification (expected within 30-60 days per state AG timelines). Document status as 'Pending Technical Root Cause Disclosure' in your incident tracking system.

4. Step 4: Recovery. If your organization shares employee or consumer PII with Plaza Home Mortgage, validate that shared data exposure is scoped correctly. Review incident tracking under NIST IR-5 (Incident Monitoring) and confirm notification obligations to affected individuals per applicable state breach notification laws.

5. Step 5: Post-Incident. Use this event to audit third-party data-sharing agreements and vendor risk posture. Reference NIST IR-8 (Incident Response Plan) to confirm your organization's third-party breach notification intake process is documented. Evaluate whether CIS 3.2 (Establish and Maintain a Data Inventory) is current enough to support rapid scope assessment in similar future events.

Detection Guidance

No confirmed IOCs, attack vectors, or technical indicators are available from current sources. Detection guidance is limited to organizational exposure assessment: (1) Determine whether your organization shares PII with Plaza Home Mortgage through data exchange, referral, or employment pipelines. (2) If a relationship exists, pull access logs and data transfer records under NIST AU-6 (Audit Record Review, Analysis, and Reporting) for the period preceding May 2026. (3) Monitor PACER, state AG breach notification portals, and Plaza Home Mortgage's official site for the formal breach notification, which will specify compromised data fields and, potentially, the attack timeline. (4) Watch for downstream phishing or social engineering targeting affected individuals if your employee population overlaps with the breach scope.

Framework Mappings

HIPAA-SECURITY

- **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
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

Sources

Source	URL	Tier
	https://www.nationalmortgagenews.com/news/plaza-home-mortgage-facin.. .	T3
Plaza Home Mortgage Data Breach Disclosed	https://www.classaction.org/data-breach-lawsuits/plaza-home-mortgag...	T3
Plaza Home Mortgage Data BreachImpacts 137976 ...	https://www.claimdepot.com/data-breach/plaza-home-mortgage-2026	T3
Plaza Home Mortgage Data Breach	https://www.reddit.com/r/Mortgages/comments/1tyn69t/plaza_home_mort...	T3
Impacted by the Plaza Home Mortgage data breach?	https://www.facebook.com/ClassActionLawsuit/posts/impacted-by-the-p...	T3

Generated 2026-06-10 15:55 UTC by TJS Security Command Center