The NAIC Data Breach: A Turning Point for Data Collection and Privacy in the Insurance Industry

Jeffrey Thomas
jthomas@mwlaw.com
(501) 688.8879

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

Laura Arp
larp@mwlaw.com
(501) 688.8885

Drew Allen
dallen@mwlaw.com
(501) 688.8813

06/29/2026

On June 17, 2026, the National Association of Insurance Commissioners (NAIC) publicly disclosed that it had identified unauthorized access to its PeopleSoft systems. The breach—attributed to the threat actor group ShinyHunters and part of a broader campaign exploiting a zero-day vulnerability in Oracle PeopleSoft—has prompted urgent responses from across the industry. Mitchell Williams previously reported on the data breach. You can read the article here.

This post examines what happened, the issues the breach has surfaced, and why this incident is likely to reshape how the insurance industry thinks about data collection, centralization, and privacy going forward.

What We Know So Far

Key developments have unfolded rapidly:

- On June 23, the NAIC expanded its disclosure, providing additional details about the scope of data potentially affected.
- On June 25, the NAIC confirmed that stolen data had been published online by ShinyHunters.
- The incident raises concerns about data governance, communication requirements, operational disruptions, and systemic risk to the regulatory framework.

Scope of Data Accessed

Based on the NAIC's disclosures to date, the data accessed included:

- Publicly available statutory financial reporting information.
- Credit rating agency data, including rating determinations of insurer investments.

The NAIC has confirmed that no personally identifiable information (PII), payment data, credit card information, or banking information was accessed.

ShinyHunters claimed to have obtained data from additional NAIC systems, including SERFF, OPTins, UCAA, EDP, and the Regulatory Data Collection (RDC) system. However, outside cybersecurity experts have confirmed that those systems were not compromised. Additionally, state insurance department systems were unaffected and producer data, policyholder information, risk-based capital data, and employee personal data were not accessed.

As of June 25, 2026, the NAIC confirmed that the stolen data has been published online by ShinyHunters. The NAIC is working with an external cybersecurity partner to compare the posted data with its own forensic analysis. The FBI is involved in the investigation.

Operational Disruptions

Beyond the data exposure itself, the breach has caused meaningful operational disruptions that underscore the insurance industry's dependence on NAIC infrastructure:

- Credit rating agencies have paused their data feeds to the NAIC, and the NAIC has temporarily suspended assigning designations to insurer investments.
- Online invoice payment via PeopleSoft remains unavailable.
- The NAIC is working with credit rating providers to provide third-party verification of systems before services resume. This process could take months.

The Hard Questions This Breach Has Raised

The NAIC breach exposed potential fault lines in how the insurance industry collects, centralizes, and governs sensitive information. The concerns raised by industry stakeholders fall into several categories, each of which is likely to be echoed in policy discussions for years to come.

Concentration Risk and Systemic Vulnerability

By aggregating regulatory filings, financial data, licensing information, examination workpapers, and other proprietary data into a single organizational target, the NAIC presents an attractive opportunity for sophisticated threat actors. Industry stakeholders have raised concerns that this concentration of data poses a structural risk to the insurance industry and to the state-based regulatory system itself.

Unanswered Questions Regarding Data Scope and Exposure

While the NAIC has confirmed that no PII or payment data was accessed, numerous questions remain unanswered regarding the full scope of data exposure. For example, inquiries have been made about which schedules and exhibits were accessed; whether information market confidential, nonpublic, trade secret or proprietary was accessed; and the total volume of data believed to have been stolen.

Containment, Forensic Transparency, and Operational Concerns

Industry participants have also raised questions regarding the forensic investigation. Questions include:

- Whether the NAIC can provide a containment statement or forensic summary from its cybersecurity experts confirming that the threat actor has been removed from the network and the situation is fully contained.
- Whether the NAIC will share an executive summary of the investigation report when completed.

The Bigger Picture: Concentration Risk and the Future of Data Governance

This incident is likely to become a defining case study in the debate over data concentration and centralized data governance in regulated industries. The NAIC maintains numerous systems that aggregate regulatory, financial, and operational data from across the entire insurance industry, including:

- CIPR (Center for Insurance Policy and Research)
- NIPR (National Insurance Producer Registry)
- SERFF (System for Electronic Rates & Forms Filing)
- SBS (State Based Systems)
- TeamMate+ (examination workpaper platform)
- Market Information Systems
- Market Conduct Annual Statement (MCAS) filings

- RIRS (Regulatory Information Retrieval System)

In aggregate, these systems represent one of the most concentrated repositories of regulatory and proprietary data in the financial services sector. The breach reminds stakeholders of the trade-off at the heart of centralized data collection: the efficiency gains of a single regulatory data hub come at the cost of creating a high-value target for increasingly sophisticated threat actors.

The breach also raises broader questions that will likely feature in future regulatory and legislative discussions: Should centralized data repositories adopt mandatory data minimization and destruction policies? Should all NAIC repositories be encrypted for all data in motion and at rest? Should data be destroyed after collection and dissemination to participating states rather than retained indefinitely? How should third-party vendor data governance standards evolve to reflect the current threat landscape?

Regulatory Implications for Insurers

One immediate consequence of the breach is that insurers themselves may face their own notification obligations. The key regulatory frameworks to consider include:

- **NAIC Insurance Data Security Model Law (#668):** Requires commissioner notification within 72 hours of determining a cybersecurity event has occurred that involves nonpublic information.
- **State Data Breach Notification Statutes:** All 50 states impose varying deadlines and requirements, with some requiring notification to Attorneys General and Consumer Reporting Agencies.
- **NYDFS 23 NYCRR Part 500:** Entities under NYDFS jurisdiction should evaluate whether notification to the Department of Financial Services is required.

Industry stakeholders have noted that licensed carriers may now have reporting requirements of their own triggered by the NAIC's breach and have requested that the NAIC provide full event information so carriers can determine whether regulatory notifications are required or whether they need to engage their own cyber insurers.

Insurers should proactively consult with counsel to assess whether the data categories confirmed as accessed—or those yet to be confirmed—may constitute "nonpublic information" or "personal information" under applicable laws triggering notification obligations.

What Insurers Should Be Doing Now

While the full implications of the NAIC breach are still unfolding, insurers should not wait for the investigation to conclude before taking action. Key steps to consider include:

- **Monitor NAIC Updates.** Continue monitoring the NAIC security update page at https://content.naic.org/about/security-update.
- **Monitor Data Publications.** Monitor whether ShinyHunters publishes additional data. NAIC is working with cybersecurity experts to compare published data with their forensic analysis.
- **Inventory Submitted Data.** Conduct a comprehensive inventory of all data submitted to the NAIC to assess potential exposure.
- **Credential Security.** Reset credentials for NAIC and insurance department systems, verify multi-factor authentication is enabled, and follow any additional NAIC guidance on portal security.
- **Review Cyber Insurance and IR Plans.** Review cyber insurance coverage and incident response plans for potential downstream impacts from a third-party breach.
- Report Suspicious Communications. Report any suspicious communications claiming to come from the NAIC to cyberincident@naic.org without responding or clicking links.

Looking Ahead

The NAIC data breach can be viewed as a stress test for the data infrastructure underpinning insurance regulation in the United States. The questions it has raised about data centralization, retention, third-party governance, and incident communication are not new, but the breach has given them an immediacy and concreteness that prior policy debates lacked.

As the investigation continues and the industry assesses the damage, this incident is likely to influence how regulators, legislators, and industry participants approach data collection and privacy for years to come. The NAIC is vital to the insurance regulatory framework and the states play an important role in overseeing the NAIC's data workflows and security. Industry and regulators alike have an interest in preserving the efficiencies NAIC data collection creates.

The situation remains fluid, and additional developments may emerge as the NAIC investigation proceeds. This post reflects information available as of June 29, 2026.