NAIC Discloses Unauthorized Access to PeopleSoft Systems

Jeffrey Thomas
jthomas@mwlaw.com
(501) 688.8879

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

Drew Allen
dallen@mwlaw.com
(501) 688.8813

06/18/2026

Cybersecurity Incident at the National Association of Insurance Commissioners (NAIC)

Overview

On June 17, 2026, the NAIC publicly disclosed that it identified unauthorized access to its PeopleSoft systems on or about June 11, 2026. The NAIC activated its incident response procedures and is working with cybersecurity experts to assess the situation. The full scope of the breach has not been determined, and the NAIC has stated it cannot yet confirm what information was affected. The NAIC's security update is available here.

Potential Impact

The NAIC maintains databases containing information submitted by insurers, producers, and other licensed entities across all 50 states, the District of Columbia, and five U.S. territories. Categories of information potentially at risk include regulatory filings, producer licensing data, financial reporting data, and personal information of NAIC personnel. Until the investigation concludes, the precise scope remains uncertain.

Notably, the threat actor group ShinyHunters has recently claimed responsibility for multiple PeopleSoft-targeted breaches in June 2026. The NAIC has not attributed this incident to any specific actor.

Key Regulatory Considerations

Depending on the content of the compromised data, notification obligations may be triggered not just under the NAIC Insurance Data Security Model Law (requiring commissioner notification within 72 hours of determining a cybersecurity event has occurred), but also state data breach notification statutes (all 50 states each imposing its own deadlines, some of which require notification to Attorneys General and to Consumer Reporting Agencies), and the NYDFS 23 NYCRR Part 500 cybersecurity regulation for entities under NYDFS jurisdiction.

Recommended Actions

We recommend that clients in the insurance industry take the following steps:

- **Monitor the NAIC's security update page** for further disclosures regarding affected data.

- **Inventory data submitted to the NAIC** to assess potential exposure, including regulatory filings, licensing information, and any personal data transmitted through NAIC systems.
- **Review breach notification obligations** under applicable state laws and the NAIC Model Law to ensure readiness to comply with notification timelines if personal information is confirmed as compromised. Companies should be prepared to reach out to insurance departments upon notice that a particular data set was or may have been compromised.
- **Reset credentials** associated with NAIC and insurance department systems and verify that multi-factor authentication is enabled.
- **Review incident response plans and cyber insurance coverage** to confirm preparedness for potential downstream impacts from this third-party breach.

We will continue to monitor this situation and provide further guidance as additional information becomes available. If you have questions about this incident or need assistance assessing potential notification obligations, please contact Jeffrey Thomas, Anton Janik, Drew Allen, or your Mitchell Williams attorney.