Series of Major Data Breaches Targeting the Insurance Industry

Client Alert | 4 min read | 08.06.25

Threat actors have targeted insurance companies in a recent string of cyber-attacks, exposing patients' personal information, including Social Security numbers, claims information, and health reports.

For example, Allianz Life Insurance Company of North America ("Allianz Life") reported a mid-July **breach** to the Maine Attorney General's Office that compromised Allianz Life's data. According to **public reports** and the regulatory filing, the threat actor gained unauthorized access to Allianz Life's systems through an external system, suggesting vulnerabilities in a third-party vendor. Since these reports, impacted individuals have filed a **class action complaint** in the U.S. District Court for the District of Minnesota, contending that Allianz Life failed to protect personal information due to negligence.

This incident comes shortly after Aflac Inc. ("Aflac"), another insurance company, **disclosed** a cybersecurity incident on July 7. The number of people impacted has not yet been reported. Erie Insurance ("Erie") also **announced** a cyber-attack earlier this summer, causing widespread disruptions that interrupted business **operations**, which included closing customer portals used to pay bills, for nearly a month.

Threat Actor Attribution: Scattered Spider

It is unclear who is behind the Allianz Life, Aflac, or Erie attacks. However, cybersecurity intelligence organizations such as **Crowdstrike** and **Mandiant**, as well as various **news sources**, have warned that the threat actor group "Scattered Spider" is focusing efforts on large U.S. enterprises in the **insurance** industry. **Scattered Spider** employs sophisticated social engineering and identity theft tactics to bypass multi-factor authentication and internal security protocols. It has been linked to previous large-scale breaches, and its tactics are part of a broader trend of cybercriminal organizations exploiting supply chain vulnerabilities and third-party relationships.

Regulatory and Legal Implications

Given the nature and scope of the data compromised, targeted insurers may face significant regulatory scrutiny from multiple authorities, including:

- State Attorneys General,
- The Federal Trade Commission (FTC), and
- The Department of Health and Human Services (HHS), if protected health information (PHI) is involved.

Additionally, companies may face:

- Class-action litigation from impacted individuals,

- Securities-related claims if disclosures related to the breach are deemed inadequate or misleading, or
- Contractual liability with third parties whose data or systems were affected.

Key Takeaways for Clients

- **Third-Party Cybersecurity Risk**: These recent attacks highlight the growing risks posed by third-party vendors. Organizations should evaluate their vendor management programs, particularly focusing on data sharing, access controls, and security certifications.
- **Incident Response Planning**: Incident response planning should be proactive. The speed and effectiveness of incident response, including timely notification, containment, and forensic analysis, plays a critical role in mitigating risk.
- **Regulatory Compliance**: Companies should ensure compliance with evolving state and federal breach notification and data privacy laws, including timely reporting and documentation practices.
- **Threat Actor Tactics Are Evolving**: Scattered Spider and similar groups are employing increasingly sophisticated techniques to circumvent traditional controls, requiring organizations to stay vigilant.

Even though they themselves are victims of a crime, companies subject to a cybersecurity incident may face significant legal and regulatory exposure. Government investigators will expect a thorough and timely response, as will internal leadership, Board Members, customers, and stakeholders.

For these reasons, targeted insurers, as well as those across industries, should consider proactive steps to address these concerns, such as:

- Conducting cybersecurity risk assessments focused on third-party vendors,
- Reviewing and updating breach notification, response, and communication protocols,
- Evaluating cyber insurance policies for adequacy and coverage, and
- Monitoring regulatory developments and litigation related to a breach for precedent-setting implications.

Crowell & Moring LLP has unparalleled experience working with companies, particularly in the insurance, health care, and technology sectors, to address these risks and continues to monitor developments.

For additional information, please contact our team.

Contacts

Laura Foggan
Partner
She/Her/Hers

Washington, D.C. D | +1.202.624.2774

lfoggan@crowell.com

Linda Malek
Partner & CHS Managing Director
New York D | +1.212.803.4069
lmalek@crowell.com

Neda M. Shaheen
Associate
She/Her/Hers

Washington, D.C. D | +1.202.624.2642
nshaheen@crowell.com

